[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 37

[Docket No. TSA-2023-0002]

RIN 1652-AA76

Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses

AGENCY: Transportation Security Administration, Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Transportation Security Administration (TSA) is proposing to amend the REAL ID regulations to waive, on a temporary and State-by-State basis, the regulatory requirement that mobile or digital driver's licenses or identification cards (collectively "mobile driver's licenses" or "mDLs") must be compliant with REAL ID requirements to be accepted by Federal agencies for official purposes, as defined by the REAL ID Act, when full enforcement of the REAL ID Act and regulations begins on May 7, 2025.

DATES: Interested persons are invited to submit comments on or before [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may submit comments, identified by the TSA docket number to this rulemaking, to the Federal Docket Management System (FDMS), a government-wide, electronic docket management system. To avoid duplication, please use only one of the following methods:

- *Electronic Federal eRulemaking Portal*: https://www.regulations.gov. Follow the online instructions for submitting comments.
- *Mail*: Docket Management Facility (M-30), U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building Ground Floor,

Room W12-140, Washington, DC 20590-0001. The Department of Transportation (DOT), which maintains and processes TSA's official regulatory dockets, will scan the submission and post it to FDMS.

- *Fax*: (202) 493-2251.

See the **SUPPLEMENTARY INFORMATION** section for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: George Petersen, Senior Program Manager, REAL ID Program, Enrollment Services and Vetting Programs, Transportation Security Administration; telephone: (571) 227-2215; email: george.petersen@tsa.dhs.gov.

Please do not submit comments to these addresses.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

TSA invites interested persons to participate in this NPRM by submitting written comments, including relevant data. Comments that will provide the most assistance to TSA will reference a specific portion of this proposed rule, explain the reason for any suggestion or recommended change, and include data, information, or authority that supports such suggestion or recommended change.

Submitting Comments

With each comment, please identify the docket number at the beginning of your comments. You may submit comments and material electronically, by mail, or fax as provided under **ADDRESSES**, but please submit your comments and material by only one means. If you submit comments by mail or in person, submit them in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you would like TSA to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard or envelope on which the docket number appears and we will mail it to you.

All comments, except those that include confidential or SSI[1] will be posted to https://www.regulations.gov, and will include any personal information you have provided. Should you wish your personally identifiable information redacted prior to filing in the docket, please clearly indicate this request in your submission. TSA will consider all comments that are in the docket on or before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Handling of Confidential or Proprietary Information and SSI Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in the **FOR FURTHER INFORMATION CONTACT** section. TSA will take the following actions for all submissions containing SSI:

- TSA will not place comments containing SSI in the public docket and will handle them with applicable safeguards and restrictions on access.
- TSA will hold documents containing SSI, confidential business information, or trade secrets in a separate file to which the public does not have access, and

[1] "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

place a note in the public docket explaining that commenters have submitted such documents.

- TSA may include a redacted version of the comment in the public docket.
- TSA will treat requests to examine or copy information that is not in the public docket as any other request under the Freedom of Information Act (5 U.S.C. 552) and the Department of Homeland Security (DHS) Freedom of Information Act regulation found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to search the electronic form of all comments in any of our dockets by the name of the individual, association, business entity, labor union, *etc*., who submitted the comment. For more about privacy and the docket, review the Privacy and Security Notice for the FDMS at https://www.regulations.gov/privacy-notice, as well as the System of Records Notice DOT/ALL 14 - Federal Docket Management System (73 FR 3316, January 17, 2008) and the System of Records Notice DHS/ALL 044 - eRulemaking (85 FR 14226, March 11, 2020).

You may review TSA's electronic public docket at https://www.regulations.gov. In addition, DOT's Docket Management Facility provides a physical facility, staff, equipment, and assistance to the public. To obtain assistance or to review comments in TSA's public docket, you may visit this facility between 9 a.m. and 5 p.m., Monday through Friday, excluding legal holidays, or call (202) 366-9826. This DOT facility is located in the West Building Ground Floor, Room W12-140 at 1200 New Jersey Avenue SE, Washington, DC 20590.

Availability of Rulemaking Document

You can find an electronic copy of this rulemaking using the Internet by accessing the Government Publishing Office's web page at https://www.govinfo.gov/app/collection/FR/to view the daily published *Federal Register*

edition or accessing the Office of the Federal Register's web page at https://www.federalregister.gov. Copies are also available by contacting the individual identified for "General Questions" in the **FOR FURTHER INFORMATION CONTACT** section.

Abbreviations and Terms Used in This Document

AAMVA-American Association of Motor Vehicle Administrators

CA/Browser Forum-Certification Authority Browser Forum

CISA-Cybersecurity and Infrastructure Security Agency

DHS-U.S. Department of Homeland Security

DID-Decentralized Identifiers

FIPS- Federal Information Processing Standards

HSM-Hardware security module

IEC-International Electrotechnical Commission

ISO-International Organization for Standardization

mDL-mobile driver's licenses and mobile identification cards

NIST-National Institute for Standards and Technology

NPRM-Notice of proposed rulemaking

PUB-Publication

RFI-Request for Information

SP-Special Publication

TSA-Transportation Security Administration

VC-Verifiable Credentials

VCDM-Verifiable Credentials Data Model

W3C-World Wide Web Consortium

Table of Contents

I. Executive Summary

A. Purpose of the Regulatory Action

B. Overview of the Proposed Rule

C. Need for a Multi-Phased Rulemaking

II. Background

A. REAL ID Act, Regulations, and Applicability to mDLs

B. Request for Information

C. mDL Overview

D. Current and Emerging Industry Standards and Government Guidelines for mDLs

E. DHS Involvement in mDLs

III. Summary of the Proposed Rule

A. Overview

B. Specific Provisions

C. Impacted Stakeholders

D. Use Cases Affected by this Proposed Rule

IV. Discussion of Public Comments in the RFI

V. Consultation with States, Non-Governmental Organizations, and the Department of Transportation

VI. Regulatory Analyses

A. Economic Impact Analyses

B. Paperwork Reduction Act

C. Federalism (E.O. 13132)

D. Customer Service (E.O. 14058)

E. Energy Impact Analysis (E.O. 13211)

F. Environmental Analysis

VII. Specific Questions

I. Executive Summary

A. Purpose of the Regulatory Action

This proposed rule is part of an incremental, multi-phased rulemaking that will culminate in the promulgation of comprehensive requirements for State issuance of REAL ID[2]-compliant mobile driver's licenses and mobile identification cards (collectively "mDLs"). In this first phase, TSA is proposing two changes to the current regulations in 6 CFR part 37, "REAL ID Driver's Licenses and Identification Cards." First, TSA is proposing to add definitions for, among others, mobile driver's licenses and mobile identification cards. These definitions provide a precise explanation of those terms as referenced in the REAL ID Act, which applies to only State-issued driver's licenses and state-issued identification cards.[3] Any other types of identification cards, such as those issued by a Federal agency, or commercial, educational, or non-profit entity, are beyond the scope of the Act and regulations. The definition of "mDL" as used in this rulemaking is limited to the REAL Act and regulations and should not be confused with "mDLs" as defined by other entities, or with State-issued mDLs that are not intended to comply with the REAL ID Act.

Second, TSA is proposing to establish a temporary waiver process that would permit Federal agencies to accept mDLs for official purposes,[4] as defined in the REAL

---

[2] The REAL ID Act of 2005, Division B of the FY05 Emergency Supplemental Appropriations Act, as amended, Public Law 109–13, 119 Stat. 302. Effective May 22, 2023, authority to administer the REAL ID program was delegated from the Secretary of Homeland Security to the Adminstrator of TSA pursuant to DHS Delegation No. 7060.2.1.

[3] *See id.* section 201 (defining a "driver's license" to include "driver's licenses stored or accessed via electronic means, such as mobile or digital driver's licenses, which have been issued in accordance with regulations prescribed by the Secretary"; mirroring definition for "identification card").

[4] The REAL ID Act defines official purposes as including but not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine. *See id.* Notably, because the Secretary has not determined any other official purposes, the REAL ID Act and regulations do not apply to Federal acceptance of driver's licenses and identification cards for other purposes, such as applying for Federal benefits programs, submitting immigration documents, or other Federal programs.

ID Act and regulations, on an interim basis when enforcement begins on May 7, 2025,[5] but only if all of the following conditions are met: (1) the mDL holder has been issued a valid and unexpired REAL ID-compliant physical driver's license or identification card from the same State that issued the mDL; (2) TSA has determined the issuing State to be REAL ID-compliant; and (3) TSA has issued a waiver to the State. To qualify for the waiver, this proposed rule would require States to submit an application demonstrating that they meet specified requirements, drawn from 19 industry and government standards guidelines. The rulemaking proposes to incorporate by reference (IBR) those standards and guidelines, which cover technical areas such as mDL communication, digital identity, encryption, cybersecurity, and network/information system security and privacy.

As noted above, this proposed rule is part of an incremental rulemaking that would temporarily permit Federal agencies to accept mDLs for official purposes until TSA issues a subsequent rule that would set comprehensive requirements for mDLs. TSA believes it is premature to issue such requirements before the May 7, 2025, deadline due to the need for emerging industry standards and government guidelines to be finalized (discussed in more detail in Part II.D., below).

The need for this rulemaking arises from TSA's desire to accommodate and foster the rapid pace of mDL innovation, while ensuring the intent of the REAL ID Act and regulations are met. Secure driver's licenses and identification cards are a vital component of our national security framework. The REAL ID Act of 2005 addressed the 9/11 Commission's recommendation that the Federal Government "set standards for the issuance of sources of identification, such as driver's licenses." Under the REAL ID Act and regulations, a Federal agency may not accept for any official purpose a State-issued driver's license or identification card, either physical or an mDL, that does not meet

[5] 88 FR 14473 (Mar. 9, 2023); DHS Press Release, DHS Announces Extension of REAL ID Full Enforcement Deadline (Dec. 5, 2022), https://www.dhs.gov/news/2022/12/05/dhs-announces-extension-real-id-full-enforcement-deadline.

specified requirements, as detailed in the REAL ID regulations (*see* part II.A., below, for more discussion on these requirements).

Although the current regulatory provisions do not include requirements that would enable States to issue REAL ID-compliant mDLs, several States are already investing significant resources to develop mDLs based on varying and often proprietary standards, many of which may lack the security, privacy, and interoperability features necessary for Federal acceptance for official purposes. The rulemaking would encourage the development of mDLs with a higher level of security, privacy, and interoperability.

Absent the proposed rule, individual States may choose insufficient mDL security and privacy safeguards that fail to meet the security purposes of REAL ID requirements and the privacy needs of users. The proposed rule would address these considerations by enabling TSA to grant a waiver to States whose mDLs TSA determines provide sufficient safeguards for security and privacy, pending completion of emerging standards. Without timely guidance from the Federal government regarding potential requirements for developing a REAL ID-compliant mDL, States risk investing in mDLs that are not aligned with emerging industry standards and government guidelines that may be IBR'd in a future rulemaking. States, therefore, may become locked-in to existing solutions and could face a substantial burden to redevelop products acceptable to Federal agencies under this future rulemaking.

Many stakeholders have already expressed these concerns to TSA. In response to an April 2021 Department of Homeland Security (DHS) Request for Information (RFI),[6] issued to inform a future rulemaking that would set technical requirements and security standards for mDLs, one commenter cautioned that the absence of a common standard "could lead to fragmentation of the market, a decrease in trust, non-interoperable

[6] *See* 86 FR 20320 (April 19, 2021).

solutions, and a global diminishing benefit of the mDL concept."[7] Similarly, another commenter warned that "[w]ithout clear, uniform, flexible standards that will encourage widespread public and private sector use of mDLs, mDLs will likely create confusion and struggle to gain a foothold in being accepted."[8]

Although this proposed rule would not set standards for the issuance of REAL ID-compliant mDLs, it does establish minimum requirements that States must meet to be granted a waiver. These proposed minimum standards and requirements would ensure that States' investments in mDLs provide minimum privacy and security safeguards consistent with information currently known to the TSA.

B. Overview of the Proposed Rule

As further discussed in part II.A., below, mDLs cannot be accepted by Federal agencies for official purposes when REAL ID full enforcement begins on May 7, 2025, unless 6 CFR part 37 is amended to address mDLs. This proposed rule would establish a process for waiving, on a temporary and State-by-State basis, the current prohibition on Federal acceptance of mDLs for official purposes, and enable Federal agencies to accept mDLs on an interim basis while the industry matures to a point sufficient to enable TSA to develop more comprehensive mDL regulatory requirements.

The current regulations prohibit Federal agencies from accepting non-compliant driver's licenses and identification cards, including both physical cards and mDLs, when REAL ID enforcement begins on May 7, 2025. Any modification of this regulatory provision must occur through rulemaking (or legislation). Until and unless TSA promulgates comprehensive mDL regulations that enable States to develop and issue REAL ID-compliant mDLs, mDLs cannot be developed to comply with REAL ID, and Federal agencies therefore cannot accept mDLs for official purposes after REAL ID

[7] Comment by American Association of Motor Vehicle Administrators.
[8] Comment by DocuSign.

enforcement begins on May 7, 2025. The proposed rule would allow the Federal government to accept mDLs on an interim basis, but only if all of the following conditions are met: (1) the mDL holder has been issued a valid and unexpired REAL ID-compliant physical driver's license or identification card, (2) TSA has determined the issuing State to be REAL ID-compliant, and (3) TSA has issued a waiver to such State based on that State's compliance with minimum privacy, safety, and interoperability requirements proposed in this rulemaking. Please see Part II.A., below, for an explanation of the REAL ID requirement that both cards and issuing States must be REAL ID compliant.

C. Need for a Multi-Phased Rulemaking

TSA recognizes both that regulations can influence long-term industry research and investment decisions and that premature regulations can distort the choices of technologies adopted, which can be costly to undo. As noted above, there are clear reasons for TSA to issue requirements for mDLs. First, there is a growing demand for and interest in mDLs due to their potential benefits of increased convenience, security, and privacy. Second, to meet this demand, States are beginning to invest in the infrastructure and programs to issue mDLs. Third, in the absence of Federal regulations and guidelines as outlined in this rulemaking, States may make unsuitable investments and issue mDLs that Federal agencies cannot accept. Fourth, adoption and use of mDLs could be thwarted if current regulations are not amended to accommodate mDLs when REAL ID enforcement begins on May 7, 2025.

At the same time, however, TSA believes it is premature to issue final, comprehensive requirements for mDLs given the rapid pace of innovation in this nascent market, and the multiple emerging industry and government standards and guidelines necessary to ensure mDL privacy and security that are still in development. From comments submitted in response to the RFI, TSA recognizes that technology and

stakeholder positions in this industry are diverse and evolving. TSA also conducted a comprehensive analysis of industry and Government standards and guidance, and the types of technology currently available. Based on this analysis, a few international industry standards applicable to mDLs are available,[9] while most are years away from publication. Accordingly, TSA has concluded that it is premature to promulgate comprehensive requirements for mDLs while those standards are emerging, because of the risk of unintended consequences, such as chilling innovation and competition in the marketplace, and "locking-in" stakeholders to certain technologies.

Although TSA believes it is premature to establish comprehensive requirements at this time, TSA believes it is appropriate to use its regulatory authority to establish a waiver process with clear standards and requirements to facilitate the acceptance of mDLs while the industry matures and moves to accepted standards. Therefore, TSA has decided to proceed with a multi-phased rulemaking approach. Initial efforts focused on research and gathering information from interested stakeholders, commencing with publication of the pre-rulemaking RFI that was intended to inform any subsequent rulemaking. "Phase 1," the current phase, would establish a temporary waiver process. This waiver process would enable secure use of mDLs when REAL ID enforcement begins on May 7, 2025, while providing TSA additional operational experience and data from TSA, which will accept mDLs during the waiver period before eventually issuing comprehensive regulations. The proposed rule is intended to serve as a regulatory bridge for this emerging technology.

Following publication of industry standards currently under development, TSA anticipates conducting a "Phase 2" rulemaking that would repeal the temporary waiver provisions, including appendix A to subpart A of the part (discussed in Part III.B.4.iv., below) established in Phase 1 and establish more comprehensive requirements enabling

[9] *See* Part II.D.

States to issue mDLs that comply with REAL ID requirements. At this time, TSA anticipates the Phase 2 rulemaking would IBR pertinent parts of some emerging standards (pending review of those final, published documents) regarding specific requirements for security, privacy, and interoperability, and distinguish between existing regulatory requirements that apply only to mDLs versus physical cards. Comments received in Phase 1, experience and data gained from temporary Federal mDL acceptance under a waiver, TSA testing of mDL acceptance at TSA airport security checkpoints, and publication of emerging standards, will inform the Phase 2 rulemaking. As one commenter[10] urged, DHS is taking "a slow and careful approach" to regulation in order to fully understand the implications of mDLs.

This iterative rulemaking approach supports Executive Order (E.O.) 14058 of December 13, 2021 (Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government), by using "technology to modernize Government and implement services that are simple to use, accessible, equitable, protective, transparent, and responsive for all people of the United States."[11] As highlighted above and discussed in more detail below, allowing acceptance of mDLs issued by States that meet the waiver requirements would enable the public to more immediately realize potential benefits of mDLs, including greater convenience, security, and privacy. *See* Part II.C.4, below, for more discussion on these benefits.

II. Background

A. REAL ID Act, Regulations, and Applicability to mDLs

The REAL ID Act of 2005 sets minimum requirements for State-issued driver's licenses and identification cards accepted by Federal agencies for official purposes, including accessing Federal facilities, boarding federally regulated commercial aircraft,

[10] *See* comment from Electronic Privacy Information Center.
[11] Published at 86 FR 71357 (Dec. 16, 2021).

entering nuclear power plants, and any other purposes that the Secretary shall determine.[12] The Act defines "driver's licenses" and "identification cards" strictly as State-issued documents,[13] and the implementing regulations, 6 CFR part 37, further refine the definition of "identification card" as "a document made or issued by or under the authority of a State Department of Motor Vehicles or State office with equivalent function."[14] Therefore, the REAL ID Act and regulations do not apply to identification cards that are not made or issued under a State authority, such as cards issued by a Federal agency or any commercial, educational, or non-profit entity.

On January 29, 2008, DHS published a final rule implementing the Act's requirements.[15] That rule included both a State compliance deadline[16] and a schedule describing when individuals must obtain a compliant driver's license or identification card intended for use for official purposes.[17] DHS refers to these two deadlines as "State-based" and "card-based" enforcement, respectively (or "full enforcement" collectively). For State-based enforcement, 6 CFR 37.65(a) prohibits Federal agencies from accepting cards issued by States and territories that are not compliant with the REAL ID standards.[18] DHS incrementally enforced the State-based deadline in phases, with the last phase beginning January 22, 2018. Since this date, many Federal agencies have accepted all valid driver's licenses and identification cards issued by REAL ID-compliant States or States with an extension or under compliance review from DHS.

---

[12] The REAL ID Act of 2005—Division B of the FY05 Emergency Supplemental Appropriations Act, as amended, Public Law 109–13, 119 Stat. 302.
[13] *Id*. at sec. 201.
[14] 6 CFR 37.3.
[15] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule, 73 FR 5272 (Jan. 29, 2008); codified at 6 CFR part 37 (2008 final rule). DHS subsequently issued six other final rules and interim final rules amending the regulations, including changes to compliance deadlines and State extension submission dates. *See* 74 FR 49308 (Sep. 28, 2009), 74 FR 68477 (Dec. 28, 2009) (final rule, stay), 76 FR 12269 (Mar. 7, 2011), 79 FR 77836 (Dec. 29, 2014); 84 FR 55017 (Oct. 15, 2019); 86 FR 23237 (May 3, 2021). In addition to final rules, DHS also published two Information Collection Requests in the Federal Register in 2016 and 2022. *See* 81 FR 8736 (Feb. 22, 2016) and 87 FR 23878 (Apr. 21, 2022).
[16] *See* 6 CFR 37.51(a).
[17] *See* 6 CFR 37.5(b).
[18] *See* 6 CFR 37.65(a).

Card-based enforcement begins on May 7, 2025.[19] On this date, Federal agencies will be prohibited from accepting for official purposes a State- or territory-issued driver's license or identification card for official purposes unless the card is compliant with the REAL ID Act and regulations.[20]

On December 21, 2020, Congress passed the REAL ID Modernization Act[21] to amend the REAL ID Act to reflect new technologies that did not exist when the law was enacted more than 15 years ago. Among other updates,[22] the REAL ID Modernization Act clarified that mDLs are subject to REAL ID requirements by amending the definitions of "driver's license" and "identification card" to specifically include mDLs that have been issued in accordance with regulations prescribed by the Secretary.[23] The REAL ID regulations therefore must be updated to distinguish which existing requirements in 6 CFR 37 apply to mDLs versus physical cards, and to include additional requirements to ensure that mDLs meet equivalent levels of security currently imposed on REAL ID-compliant physical cards and are otherwise secure. An mDL cannot be REAL ID-compliant until TSA establishes REAL ID requirements in regulations and States issue mDLs compliant with those requirements. As a result of this requirement, mDLs must also be REAL ID-compliant to be accepted when card-based enforcement begins on May 7, 2025.

B. Request for Information

In April 2021, DHS issued an RFI announcing DHS's intent to commence future rulemaking to set the minimum technical requirements and security standards for mDLs to enable Federal agencies to accept mDLs for official purposes. The RFI requested

---

[19] *See* 6 CFR 37.5(b).
[20] See *id*.
[21] REAL ID Modernization Act, Title X of Division U of the Consolidated Appropriations Act, 2021, Public Law 116-260, 134 Stat. 2304.
[22] TSA is conducting a separate rulemaking to implement other sections of the REAL ID Modernization Act.
[23] Sec. 1001 of the REAL ID Modernization Act, Title X of Division U of the Consolidated Appropriations Act, 2021, Public Law 116-260, 134 Stat. 2304.

comments and information to inform DHS's rulemaking.[24] In June 2021, DHS held a public meeting to provide an additional forum for comment.[25] In response to comments at the public meeting concerning the importance of public access to an industry-developed standard referenced in the RFI, DHS subsequently published a notification in the *Federal Register* to facilitate access to the standard.[26] DHS also conducted extensive outreach and engagement with affected stakeholders, including States, industry, and individuals. DHS also conducted a roundtable discussion on privacy considerations with non-profit organizations representing varied interests.

The RFI requested comments on 13 specific topics, including: potential security risks arising from mDL usage and mitigating solutions, potential privacy concerns or benefits associated with mDL transactions, the maturity of certain industry standards and the appropriateness of DHS's adoption of them, costs to individuals to obtain mDLs, and various technical topics associated with mDL issuance and communications. In response, DHS received about 60 comments. Please see Part IV, below, for a detailed discussion of the comments received, which are also referenced throughout this preamble.

C. mDL Overview

1. mDLs Generally

Driven by increasing public demand for more convenient, secure, and privacy-enhancing forms of identification, many States have invested significantly and rapidly in recent years to develop mDL technology. An mDL is generally recognized as the digital representation of an individual's identity information contained on a State-issued physical driver's license or identification card.[27] An mDL may be stored on a diverse range of

[24] 86 FR 20320 (April 19, 2021).
[25] 86 FR 31987 (June 16, 2021).
[26] 86 FR 51625 (Sept. 16, 2021).
[27] A technical description of mDLs as envisioned by the American Association of Motor Vehicle Administrators may be found at https://www.aamva.org/Mobile-Drivers-License/.

portable or mobile electronic devices, such as smartphones, smartwatches, and storage devices containing memory. Like a physical card, mDL data originates from identity information about an individual that is maintained in the database of a State driver's licensing agency.

Unlike physical driver's licenses that are read and verified visually through human inspection of physical security features, an mDL is read and verified electronically using a device known simply as a "reader" (discussed in Part II.C.2., below). Physical cards employ physical security features to deter fraud and tampering, such as "easily identifiable visual or tactile [security] features" on the surface of a card.[28] An mDL, in contrast, combats fraud through the use of digital security features that are not recognizable through human inspection. For example, mDLs usually rely on digital security through use of asymmetric cryptography/public key infrastructure (PKI). As discussed in the RFI,[29] Asymmetric cryptography generates a pair of encryption "keys" to encrypt and decrypt protected data. One key, a "public key," is distributed publicly, while the other key, a "private key," is held by the State driver's licensing agency (i.e., a Department of Motor Vehicles, or "DMV"). When a DMV issues an mDL to an individual (see Fig. 1, below, communication no. 1), the DMV uses its private key to digitally "sign" the mDL data. A Federal agency validates the integrity of the mDL data by obtaining the DMV's public key to verify the digital signature (see Fig. 1: mDL Secure Communications). Private keys and digital signatures are elements of data encryption that protect against unauthorized access, tampering, and fraud.

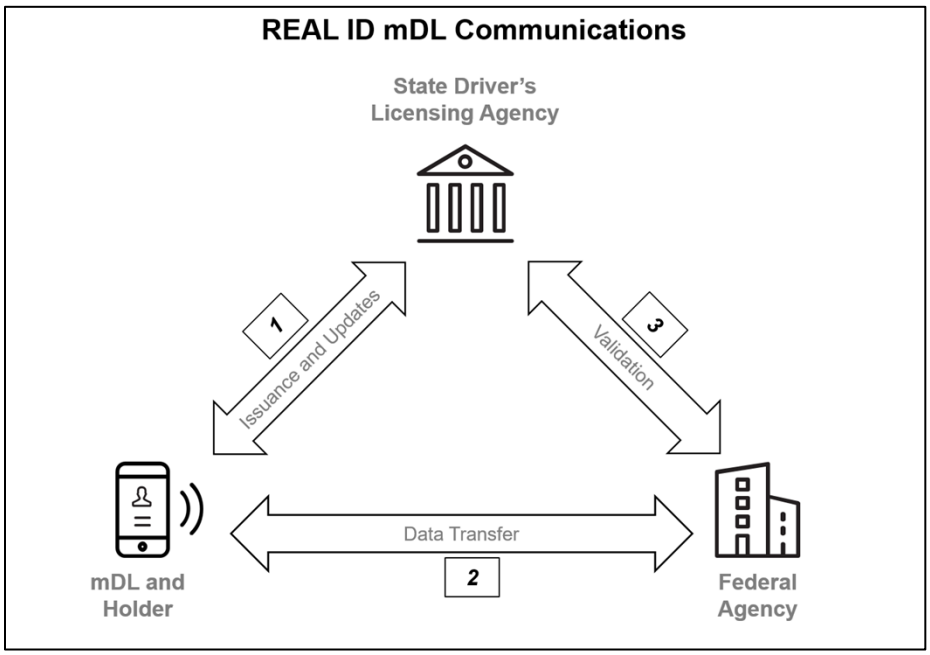
Generally, mDL-based identity verification under REAL ID would involve a triad of secure communications between a State driver's licensing agency, an mDL holder, and a Federal agency. Specifically, and as shown in Fig. 1, below, the following three

---

[28] 6 CFR 37.15(c) and 37.17(h).
[29] *See* 86 FR 20320, 20324 (April 19, 2021).

communications would occur: (1) Issuance and Updates: the DMV would issue or "provision" an mDL onto a mobile device of the person requesting the mDL (who then becomes the mDL holder), (2) Data Transfer: the mDL holder would authorize release of relevant data from the device to a Federal agency, which would use a reader to retrieve data, and (3) Validation: the Federal agency would use a reader, to confirm that the data originated from the issuing DMV and is unchanged, by verifying the DMV's public key. Although not depicted in Fig. 1, the Federal agency would also validate (via human inspection or facial matching software) that the mDL belongs to the individual presenting it by comparing the individual's live appearance to the photo retrieved by the reader. Standardized communication interfaces are necessary to enable Federal agencies to exchange information with all 56 U.S. States and territories that issue mDLs.

Fig. 1: mDL Secure Communications



2. mDL Readers

Any Federal agency that chooses to accept mDLs for REAL ID official purposes would need to procure and use readers to validate an mDL holder's identity data from their mobile device and establish trust that the mDL is secure by using private-public key data encryption. Non-Federal agencies, such as State agencies, businesses, and other

entities who choose to accept mDLs for uses beyond the scope of REAL ID are not governed by the REAL ID Act or regulations and therefore would make their own independent decisions concerning reading mDLs and reader procurement.[30] The reader would confirm that the mDL holder's identity data is valid by performing the following steps: establishing a secure digital connection with an mDL holder's mobile device, receiving the required mDL information for identity verification, verifying its authenticity and integrity by validating the driver's licensing agency's digital signature of the mDL data, and confirming that the mobile device possesses the unique device key corresponding to the mDL at the time of issuance.

An mDL reader can take multiple forms, ranging from software to hardware. In its simplest form, an mDL reader can be an app installed on a smartphone or other mobile device. A reader could also be a dedicated device. This is expected to be a low-cost solution that could be added to existing smartphones carried by a verifying entity's employee. While reader development is ongoing in the industry, TSA understands that companies are already beginning to offer verification apps for free on their commercial app stores. As reader technology continues to evolve, there will likely be wide range of reader options with various capabilities and associated price points.[31]

3. State mDL Issuance

---

[30] Non-Federal agencies and other entities who choose to accept mDLs for uses beyond the scope of REAL ID should also recognize the need for a reader to ensure the validity of the mDL. Any verifying entity can validate in the same manner as a Federal agency if they implement the standardized communication interface requirements specified in this proposed rule, which would require investment to develop the necessary IT infrastructure and related proceses.

[31] Readers for mDLs have specific requirements and at this time are not interchangeable with readers for other types of Federal cards, such as the Transportation Worker Identification Credential (TWIC). Although TSA is evaluating some mDLs at select airport security checkpoints (see Part II.E.), cost estimates for readers used in the evaluations are not available because those readers are non-commercially available prototypes designed specifically for integration into TSA-specific IT infrastructure that few, if any, other Federal agencies use. In addition, mDL readers are evolving and entities who accept mDLs would participate voluntarily. Accordingly, associated reader costs are not quantified at this time but TSA intends to gain a greater understanding of any costs to procure reader equipment as the technology continues to evolve.

As noted above, mDL-issuance is proliferating rapidly among States, with nearly half of all States piloting, issuing, or considering mDLs. As of the date of this NPRM, at least eight States (Arizona, Colorado, Delaware, Louisiana, Maryland, Mississippi, Oklahoma, and Utah) are issuing mDLs, and three States (Florida, Iowa, and Virginia) are currently piloting or have piloted mDLs. Additionally, at least 17 States (California, District of Columbia, Georgia, Hawaii, Illinois, Indiana, Kentucky, Michigan, Missouri, New Jersey, New York, North Dakota, Pennsylvania, Puerto Rico, Tennessee, Texas, and Wyoming) have indicated they are studying mDLs or considering enabling legislation.

Based on its analysis of the current environment, TSA believes that States are issuing mDLs using widely varying technology solutions, resulting in a fragmented environment rather than a common standard for issuance and use. The various States issuing or piloting mDLs are believed to be using technology solutions provided by multiple vendors, and it is not clear whether such technological diversity provides the safeguards and interoperability necessary for Federal acceptance. For example, in September 2021 and March 2022, Apple announced[32] that it was working with 13 States (Arizona, Colorado, Connecticut, Georgia, Hawaii, Iowa, Kentucky, Maryland, Mississippi, Ohio, Oklahoma, Puerto Rico, and Utah) to enable their mDLs to be provisioned into Apple's Wallet app. Google and GET Group North America have made similar announcements.[33] States choosing a variety of technology solutions, which could result in non-standard, non-compatible technologies, which raises additional questions concerning the Federal government's ability to accept the mDLs for Federal purposes.

Although detailed mDL adoption statistics are unavailable, anecdotal information and fragmented reporting indicates that mDLs are rapidly gaining public acceptance. For

---

[32] https://www.apple.com/newsroom/2021/09/apple-announces-first-states-to-adopt-drivers-licenses-and-state-ids-in-wallet/; https://www.apple.com/newsroom/2022/03/apple-launches-the-first-drivers-license-and-state-id-in-wallet-with-arizona/.

[33] https://support.google.com/wallet/answer/12436402?hl=en; https://getgroupna.com/get-mobile-id-is-now-accepted-at-tsa-precheck/.

example, Louisiana has recently reported that over one million residents (representing more than 20% of its population) have installed Louisiana's mDL app on their mobile devices.

4. Potential Benefits of mDLs

An mDL has potential benefits for all stakeholders. For Federal agencies that require REAL ID-compliant IDs for official purposes, mDLs may provide efficiency and security enhancements. Compared to physical cards, which rely on manual inspection of physical security features on the surface of a card designed to deter tampering and fraud, mDLs rely on digital security features that are immune to many vulnerabilities of physical security features. For individuals, some commenters noted that mDLs may provide a more secure, convenient, privacy-enhancing, and "touchless" method of identity verification compared to physical IDs.[34] Among other privacy-enhancing features, the holder of an mDL could control what data fields are released. For example, if an mDL is used for identity purposes with a Federal agency, the holder could restrict the agency to receiving only the data necessary and required by the agency to verify the individual's identity. Potential hygiene benefits also derive from the contact-free method of ID verification enabled by mDLs. An mDL holder may transmit data to a verifying Federal agency's mDL reader by hovering their mDL above the reader, potentially eliminating any physical contact with the individual's mobile device thereby reducing germ transmission.

D. Current and Emerging Industry Standards and Government Guidelines for mDLs

The nascence of mDLs and absence of standardized mDL-specific requirements provide an opportunity for industry and government to develop standards and guidelines to close this void. TSA is aware of multiple such documents, both published and under

[34] *See, e.g.,* comments submitted by: Applied Recognition, Bredemarket, Hiday, Mothershed, Muller, State of Connecticut, DHS of Motor Vehicles, Secure Technology Alliance, U.S. Travel Association.

development, from both Federal and non-government sources. This section discusses standards and guidelines that form the basis of many of the requirements proposed in this rulemaking, as well as additional documents that may inform the upcoming Phase 2 rulemaking. As discussed in Part III.B.8, below, this rulemaking proposes to amend § 37.4 by incorporating by reference into part 37 nineteen standards and guidelines. All proposed incorporation by reference material is available for inspection at DHS Headquarters in Washington D.C., please email requesttoreviewstandards@hq.dhs.gov. The material may also be obtained from its publisher, as discussed below.

1. American Association of Motor Vehicle Administrators

In September 2022, the American Association of Motor Vehicle Administrators published mDL Implementation Guidelines (AAMVA Guidelines). *Mobile Driver's License (mDL) Implementation Guidelines Version 1.2* (Jan. 2023), American Association of Motor Vehicle Administrators, 4401 Wilson Boulevard, Suite 700, Arlington, VA 22203, available at https://aamva.org/getmedia/b801da7b-5584-466c-8aeb-f230cef6dda5/mDL-Implementation-Guidelines-Version-1-2_final.pdf. The Guidelines are available to the public for free at the link provided above. The AAMVA Guidelines adapt industry standard ISO/IEC 18013-5:2021 (discussed in Part II.D.4., below), for State driver's licensing agencies through the addition of more stringent and more specific recommendations, as the ISO/IEC standard has been developed for international purposes and may not meet all purposes and needs of States and the Federal Government. For example, Part 3.2 of the AAMVA Guidelines modify and expand the data elements specified in ISO/IEC 18013-5:2021, in order to enable the mDL to indicate the REAL ID compliance status of the companion physical card, as well as to ensure interoperability necessary for Federal acceptance. AAMVA has added data fields for DHS Compliance and DHS Temporary Lawful Status. These additional fields provide the digital analog to the requirements for data fields for physical cards defined in 6 CFR

37.17(n)[35] and 37.21(e)[36] respectively. As discussed generally in Part III.B, below, § 37.10(a)(1) and (4) of this proposed rule would require a State to explain, as part of its application for a waiver, how the State issues mDLs that are compliant with specified requirements of the AAMVA Guidelines.

2. Certification Authority Browser Forum

The Certification Authority Browser Forum (CA/Browser Forum) is an organization of vendors of hardware and software used in the production and use of publicly trusted certificates. These certificates are used by forum members, non-member vendors, and governments to establish the security and trust mechanisms for public key infrastructure-enabled systems. The CA/Browser Forum has published two sets of requirements applicable for any implementers of PKI, including States that are seeking to deploy Certificate Systems that must be publicly trusted and used by third parties:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.8.6 (December 14, 2022), available at https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.6.pdf, and
- Network and Certificate System Security Requirements v. 1.7 (April 5, 2021), available at https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf. CA/Browser Forum, 815 Eddy St, San Francisco, CA 94109, (415) 436-9333.

These documents are available to the public for free at the links provided above.

---

[35] Section 37.17(n) provides, "The card shall bear a DHS-approved security marking on each driver's license or identification card that is issued reflecting the card's level of compliance as set forth in § 37.51 of this Rule."

[36] Section 37.21(e) provides, "Temporary or limited-term driver's licenses and identification cards must clearly indicate on the face of the license and in the machine readable zone that the license or card is a temporary or limited-term driver's license or identification card."

To issue mDLs that can be trusted by Federal agencies, each issuing State must establish a certificate system, including a root certification authority that is under control of the issuing State. TSA believes the CA/Browser Forum requirements for publicly trusted certificates have been proven to be an effective model for securing online transactions. As discussed generally in Part III.B.4, below, appendix A to subpart A of the part, sections 1, 2, and 4-8, require compliance with specified requirements of the CA/Browser Forum Baseline Requirements and/or Network and Certificate System Requirements. Section 37.4 of this proposed rule would IBR these CA/Browser Forum references.

3. Cybersecurity Guidelines

DHS and the Cybersecurity and Infrastructure Security Agency (CISA) have published two guidelines which are relevant to the operations of States' mDL issuance systems:

- National Cyber Incident Response Plan (Dec. 2016), available at https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf, and
- CISA Cybersecurity Incident & Vulnerability Response Playbooks (Nov. 2021), available at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

Cybersecurity and Infrastructure Security Agency, Mail Stop 0380, 245 Murray Lane, Washington, D.C. 20528-0380, (888) 282-0870. These guidelines, available for free at the links provided above, provide details on best practices for management of systems during a cybersecurity incident, providing recommendations on incident and vulnerability response. Management of cybersecurity incidents and vulnerabilities are critical to maintenance of a State's mDL issuance information technology (IT) infrastructure. As

discussed generally in Part III.B.4, below, appendix A to subpart A of the part, section 8, requires compliance with specified requirements of the DHS National Cyber Incident Response Plan and the CISA Cybersecurity Incident & Vulnerability Response Playbooks. Section 37.4 of this proposed rule would IBR these DHS and CISA standards.

4. ISO/IEC Standards and Technical Specifications

Two international standards-setting organizations, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC),[37] are jointly drafting two series of multi-part International Standards and Technical Specifications.[38] Series ISO/IEC 18013, *Personal identification — ISO-compliant driving licence* Parts 5-7, are specific to mDLs, and series ISO/IEC 23220 *Cards and security devices for personal identification — Building blocks for identity management via mobile devices*, Parts 1-6, concern digital identity (of which mDLs are a subset). DHS TSA has participated in the development of both Series as a non-voting member of the United States national body member of the Joint Technical Committee.[39] Together, both Series would establish standardized interfaces that would enable the mDL communications triad (see Part II.C.1., above) as follows: (1) State driver's licensing

---

[37] ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies. ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. The IEC publishes consensus-based international standards and manages conformity assessment systems for electric and electronic products, systems and services, collectively known as "electrotechnology." ISO and IEC standards are voluntary and do not include contractual, legal or statutory obligations. ISO and IEC standards contain both mandatory requirements and optional recommendations, and those who choose to implement the standards must adopt the mandatory requirements.

[38] ISO defines an International Standard as "provid[ing] rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context. It can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards." www.iso.org/deliverables-all.html. In contrast, ISO defines a "Technical Specification" as "address[ing] work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard." www.iso.org/deliverables-all.html.

[39] A member of the TSA serves as DHS's representative to the Working Group.

agency and the mDL holder (Series 23220), (2) mDL Holder and a verifying entity (Series 18013), and (3) verifying entity and State licensing agency (Series 18013).

In September 2021, ISO and IEC published international standard ISO/IEC 18013, Part 5, entitled, "Personal identification – ISO-compliant driving licence." ISO/IEC 18013-5:2021, *Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application* (Sept. 2021), International Organization for Standardization, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland, +41 22 749 01 11, www.iso.org/contact-iso.html.[40] Section 37.4 of this rulemaking proposes to IBR this standard, which is available from DHS as discussed above. In addition, the American National Standards Institute (ANSI), a private organization not affiliated with DHS, will provide public access[41] to ISO/IEC 18013-5:2021 until [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Standard ISO/IEC 18013-5:2021 standardizes the interface between an mDL and an entity seeking to read an individual's mDL for identify verification purposes, and sets full operational and communication requirements for both mDLs and mDL readers. This standard applies to "attended" mode verification, in which both the mDL holder and an officer or agent of a verifying entity are physically present together during the time of identity verification.[42] DHS received numerous comments in response

---

[40] Forthcoming Part 6 of Series ISO/IEC 18013, "mDL test methods," is a technical specification that will enable testing of mDLs and readers to certify conformance with ISO/IEC 18013-5:2021. TSA anticipates a draft of this standard may be completed by the end of 2023, and the final document may publish at the end of 2024.

[41] ANSI advises interested persons to visit the following website to obtain access: https://www.surveymonkey.com/r/DQVJYMK. This link will direct interested persons to a nongovernment website that is not within the Federal government's control and may not follow the same privacy, security, or accessibility policies as Federal government websites. ANSI requires individuals to complete an online license agreement form, which will ask for name, professional affiliation, and email address, before it grants access to any standards. ANSI will provide access on a view-only basis, meaning copies of the document cannot be downloaded or modified. Individuals who access non-governmental sites to view available standards are subject to the policies of the owner of the website. For access to non-final draft standards, please contact ISO/IEC using the information provided earlier.

[42] Part 7 of Series ISO/IEC 18013, entitled "mDL add-on function," is an upcoming technical specification that will standardize interfaces for "unattended" mode verification, in which the mDL holder and officer/agent of the verifying agency are not physically present together, and the identity verification is conducted remotely. Unattended identity verification is not currently considered a REAL ID use case.

to the RFI concerning the appropriateness of this standard as a starting point for future regulatory requirements.[43] Many comments received in response to the RFI noted that standard ISO/IEC 18013-5:2021, which published in Sept. 2021, provides a sufficient baseline for secure Federal acceptance.[44] After carefully considering all comments received, TSA believes ISO/IEC 18013-5:2021 is critical to enabling the interoperability, security, and privacy necessary for wide acceptance of mDLs by Federal agencies for official purposes. As discussed in Part III.B, below, this NPRM proposes to IBR this standard into part 37. Specifically, § 37.8 of the proposed rule would require Federal agencies to validate an mDL as required by standard ISO/IEC 18013-5:2021, and § 37.10(a)(4) would require a State to explain, as part of its application for a waiver, how the State issues mDLs that are interoperable with this standard to provide the security necessary for Federal acceptance.

The ISO/IEC 23220 Series of Technical Specifications, "Cards and security devices for personal identification – Building blocks for identity management via mobile devices," cover international digital IDs broadly and are applicable to mDLs. ISO/IEC 23220: *Cards and security devices for personal identification — Building blocks for identity management via mobile devices*, International Organization for Standardization, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland, +41 22 749 01 11, www.iso.org/contact-iso.html. This Series consists of six Parts, with Parts 3, 5, and 6 being relevant to mDLs and the forthcoming Phase 2 rulemaking. More specifically,

---

[43] *See, e.g.*, comments submitted by: American Association of Motor Vehicle Administrators; American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center; Apple; Association for Convenience & Fuel Retailing; CBN Secure Technologies; FaceTec; Florida DHS of Highway Safety and Motor Vehicles; IDEMIA; Maryland DHS of Transportation, Motor Vehicle Administration; National Immigration Law Center and Undersigned Organizations; Secure Technology Alliance; State of Connecticut, DHS of Motor Vehicles; Underwriters Laboratories; Verifiable Credentials Policy Committee, Blockchain Advocacy Coalition. All comments are available at https://www.regulations.gov/docket/DHS-2020-0028.

[44] *See* comments submitted by American Association of Motor Vehicle Administrators; Florida DHS of Highway Safety and Motor Vehicles; Maryland DHS of Transportation, Motor Vehicle Administration; State of Connecticut, DHS of Motor Vehicles.

Series 23220 would establish the following critical requirements for "provisioning"[45] an mDL, which refers to the various steps required for a State driver's licensing agency to securely place an mDL onto a mobile device:

- Part 3, "Protocols and services for installation and issuing phase," covers data function calls and formatting that States will use to communicate (*e.g.,* provision, refresh, revoke) with a mobile device.
- Part 5, "Trust models and confidence level assessment," covers trust framework and provisioning, including confidence levels, identity proofing, binding, identity resolution, evidence validation, evidence verification, and holder authentication.
- Part 6, "Mechanism for use of certification on trustworthiness of secure area," primarily covers device security requirements and trust of the secure areas in mobile devices.

TSA anticipates that Series ISO/IEC 23220 will define critical requirements for the interface between a State driver's licensing agency and mobile device. However, none of Parts 3, 5, and 6 of Series 23220 have published. TSA understands that drafts of Parts 3 and 5 may publish in late 2023, and final publication is possible by the end of 2024; publication dates for Part 6 are unknown, but a draft is anticipated in 2024. DHS received many comments in response to the RFI cautioning, however, that standard ISO/IEC 23220, Parts 3, 5, and 6, are not sufficiently mature to inform regulatory requirements.[46] Given the evolving stage of Series ISO/IEC 23220 and comments to the RFI, TSA believes it is premature to rely on this Series to inform this proposed rulemaking and thus is not proposing to IBR them in this NPRM. TSA may consider

[45] The initial step of provisioning requires proving that an mDL applicant owns the mobile device onto which the mDL will be stored. Next, a trusted connection would be established between the licensing agency and the target device. Finally, the licensing agency would use this connection to securely transmit and update mDL data on the device.

[46] *See* comments submitted by American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center; IDEMIA; Maryland DHS of Transportation, Motor Vehicle Administration; Underwriters Laboratories.

adopting requirements of pertinent Parts of this standard in the upcoming Phase 2 rulemaking, pending review of the final published documents.

5. National Institute for Standards and Technology

i. Digital Identity Guidelines

The National Institute for Standards and Technology (NIST) has published Digital Identity Guidelines, NIST SP 800-63-3, that cover technical requirements for Federal agencies implementing digital identity. NIST Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017), National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. The Digital Identity Guidelines, available for free at the link provided above, define technical requirements in each of the areas of identity proofing, registration, user authentication, and related issues. Because TSA is not aware of a common industry standard for mDL provisioning that is appropriate for official REAL ID purposes today, TSA views the current NIST Digital Guidelines as critical to informing waiver application requirements for States regarding provisioning (discussed in detail in Part III.B.4., below). As discussed generally in Part III.B.4**,** below**,** under proposed rule text § 37.10(a)(2), which requires compliance with appendix A to subpart A of the part, a State must explain, as part of its application for a waiver, how the State issues mDLs that are compliant with NIST SP 800-63-3 to provide the security for mDL IT infrastructure necessary for Federal acceptance. Section 37.4 of this proposed rule would IBR NIST SP 800-63-3.

NIST has also published Digital Identity Guidelines Authentication and Lifecycle Management, NIST SP 800-63B, as a part of NIST SP 800-63-3. NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management* (June 2017), National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899, available at

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf. This document provides technical requirements for Federal agencies implementing digital identity services. The standard focuses on the authentication of subjects interacting with government systems over open networks, establishing that a given claimant is a subscriber who has been previously authenticated and establishes three authenticator assurance levels. As discussed generally in Part III.B.4, below, proposed rule text § 37.10(a)(2) requires compliance with appendix A to subpart A of the part, which would require a State to explain, as part of its application for a waiver, how the State manages its mDL issuance infrastructure using authenticators at assurance levels provided in NIST SP 800-63B. Section 37.4 of this proposed rule would incorporate by reference NIST SP 800-63B.

NIST is developing a revision to the Digital Identity Guidelines, SP 800-63-4, which is expected to impact key issues related to mDL processes. This publication and its companion volumes NIST SP 800-63A Rev. 4, SP 800-63B Rev. 4, and SP 800-63C Rev. 4, provide technical guidelines for the implementation of digital identity services. Initial public drafts of this suite published in December 2022, and final drafts may publish in early 2024. The full suite of draft NIST Digital Identity Guidelines, NIST SP 800-63-4, are available for free as follows:

- NIST SP 800-63-4, *Digital Identity Guidelines, Initial Public Draft* (December 2022), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf.
- NIST SP 800-63A Rev. 4 *Digital Identity Guidelines: Enrollment and Identity Proofing, Initial Public Draft* (December 2022), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.ipd.pdf;

- NIST SP 800-63B Rev. 4 *Digital Identity Guidelines: Authentication and Lifecycle Management, Initial Public Draft* (December 2022), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.ipd.pdf;
- NIST SP 800-63C Rev. 4 *Digital Identity Guidelines: Federation and Assertions, Initial Public Draft* (December 2022), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63C-4.ipd.pdf.

National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899. The final versions of these publications may be candidates for incorporation by reference (pending review of the final published documents) in the forthcoming Phase 2 rulemaking.

ii. Federal Information Processing Standards

NIST also maintains the Federal Information Processing Standards (FIPS) which relate to the specific protocols and algorithms necessary to securely process data. This suite of standards includes:

- NIST FIPS PUB 140-3, Security Requirements for Cryptographic Modules (March 22, 2019), available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf,
- NIST FIPS PUB 180-4, Secure Hash Standard (SHS) (August 4, 2015), available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf,
- NIST FIPS PUB 186-5, Digital Signature Standard (DSS) (February 3, 2023), available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf,
- NIST FIPS PUB 197, Advanced Encryption Standard (AES) (November 26, 2001) available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf,

- NIST FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC) (July 16, 2008) available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf, and
- NIST FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (August 4, 2015) available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.

National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899. This suite of FIPS standards, available for free at the links provided above, are critical to the transactions required for mDLs, and any Federal systems which interact with or are used to verify a mDL for REAL ID official purposes will be required to use the algorithms and protocols defined. As discussed generally in Part III.B, below, § 37.10(a)(4) requires compliance with specified requirements of NIST FIPS PUB 180-4, 186-5, 197, 198-1, and 202, and appendix A to subpart A of the part, section 5, requires compliance with FIPS PUB 140-3. Section 37.4 of this proposed rule would incorporate by reference the suite of FIPS standards discussed above.

iii. Security and Privacy Controls for Information Systems and Organizations; Key Management

NIST has published several guidelines to protect the security and privacy of information systems:

- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations (September 2020), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
- NIST SP 800-57 Part 1, Rev. 5, Recommendation for Key Management: Part 1 – General (May 2020), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

- NIST SP 800-57 Part 2, Rev. 1, Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations (May 2019), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf.
- NIST SP 800-57 Part 3, Rev. 1, Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance (January 2015) available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf.

National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899. All of these documents are available for free at the links provided above.

Collectively, NIST SP 800-53 Rev. 5 and NIST SP 800-57 provide relevant controls for States regarding mDL security and privacy covering a broad range of topics related to the administration of a certificate system including: access management; certificate life-cycle policies; operational controls for facilities and personnel; technical security controls; and vulnerability management such as threat detection, incident response, and recovery planning. Due to the sensitive nature of State Certificate System processes and the potential for significant harms to security if confidentiality, integrity, or availability of the certificate systems is compromised, the minimum risk controls specified in appendix A to subpart A of the part require compliance with the NIST SP 800-53 Rev. 5 "high baseline" as set forth in that document, as well as compliance with the specific risk controls described in the appendix. In addition, and as discussed generally in Part III.B, below: appendix A to subpart A of the part, secs. 1-8, require compliance with NIST SP 800-53 Rev. 5; secs. 1 and 5 require compliance with NIST SP 800-57 Part 1, Rev. 5; sec. 1 requires compliance with NIST SP 800-57 Part 2 Rev. 1; and sec. 1 requires compliance with NIST SP 800-57 Part 3, Rev. 1. Section 37.4 of this proposed rule would incorporate by reference NIST SP 800-53 Rev. 5 and the full suite of NIST SP 800-57 references discussed above.

iv. Cybersecurity Framework

NIST has published the Framework for Improving Critical Infrastructure Cybersecurity v. 1.1 (April 16, 2018), National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. This document, available for free at the link provided above, provides relevant information for cybersecurity for States issuing mDLs. As discussed generally in Part III.B., below, certain requirements from the NIST Cybersecurity Framework have been adopted in appendix A to subpart A of the part, secs. 1,2, 5-8. Section 37.4 of this proposed rule would incorporate by reference the NIST Cybersecurity Framework.

6. W3C Standards

In its RFI, DHS specifically sought comments on industry standards that could inform future regulatory requirements.[47] DHS received multiple comments[48] concerning standards being developed by the World Wide Web Consortium (W3C), which is a standards-development organization that develops open standards for the World Wide Web. Similar to its involvement with ISO, DHS has participated in the development of these standards as a non-voting member in the W3C Credential Community Group.

While TSA is not proposing to IBR these W3C standards in this NPRM, TSA understands that W3C is developing two standards concerning digital identification that, like the ISO/IEC Series of standards discussed above, may be relevant to the Phase 2 rulemaking. The W3C standards are "Verifiable Credentials Data Model v1.1" (VCDM v1.1) and "Decentralized Identifiers v1.0" (DID v1.0). *Verifiable Credentials Data Model v1.1* (March 3, 2022), W3C/MIT, 105 Broadway, Room 7-134, Cambridge, MA

[47] 86 FR 20320 at 20325-26.

[48] *See* comments submitted by American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center; Association for Convenience & Fuel Retailing; CBN Secure Technologies; Indico.tech and Lorica Identity; Mastercard; Muller; OpenID Foundation; UL; Verifiable Credentials Policy Committee, Blockchain Advocacy Coalition.

02142, available at www.w3.org/TR/vc-data-model/; *Decentralized Identifiers (DIDs) v1.0* (July 19, 2022), W3C/MIT, 105 Broadway, Room 7-134, Cambridge, MA 02142, available at www.w3.org/TR/did-core/. These documents are available to the public for free at the links provided above. DHS has participated in the development of these standards as a non-voting member in the W3C Credential Community Group.

In March 2022, the W3C published VCDM v1.1. A "Verifiable Credential" (VC) is a form of digital identification, developed under this standard, with features that enable a verifying entity to confirm its authenticity.[49] This standard defines elements of a data model that enables using a digital identity in online transactions. The standard appears to provide broad requirements that enable issuance of diverse types of secure digital identification using varying data fields (e.g., name, date of birth), data types (e.g., text, numeric values, length of data string), and methods of digital security. Although the standard sets forth specifications for the data model generally, TSA understands the standard does not provide specific requirements to implement security and privacy protections for the data model. Instead, references to these topics appear to be largely non-binding, informative guidance. For example, the standard requires that the VC contain at least one encryption mechanism to detect tampering (such as a digital signature), but does not set forth any specific mechanisms that are acceptable. [50] Similarly, although the standard encourages the use of mechanisms to enable a VC holder to selectively release only certain data to a verifying entity, it does not specify acceptable implementation mechanisms.[51]

In July 2022, W3C published complementary standard DID v1.0, which specifies the essential requirements to enable the use of diverse types of digital identification in online transactions. A "DID," is a unique identifier used in online transactions that, for

---

[49] *See* VCDM sections 1 and 2.
[50] *See* VCDM sections 4.7 and 8.1.
[51] *See* VCDM sections 5.8 and 7.8.

example, enables VC holders to authenticate themselves. A DID can be used in a blockchain system. Like the VCDM standard, DHS understands that the DIDs standard includes non-binding guidance, but no prescriptive specifications, concerning security and privacy.

In their current forms, TSA understands that the W3C VCDM standard and DID standard focus on the use of digital identification in unattended mode internet transactions, which is different from the attended, in-person REAL ID transactions contemplated for mDLs under this rulemaking. In addition, the current versions of the W3C standards do not set forth specific requirements concerning security and privacy or an mDL-specific data model, which may impede States from developing standardized, interoperable mDLs. Several commenters also expressed similar concerns.[52] TSA is not aware of any State pursuing an mDL with the VCDM model as the sole data model. However, TSA understands that W3C's work is ongoing, and future revisions may set forth security, privacy requirements, interoperability requirements, and a standardized data model needed for in-person REAL ID identity verification. In addition, given the breadth of the VCDM and DID, it may be possible in the future to develop a VCDM-based mDL that conforms to both W3C recommendations and the ISO/IEC standards simultaneously, providing full ecosystem interoperability. As stated above, TSA is not proposing to IBR these W3C Standards in this NPRM.

TSA understands that the standards and guidelines discussed above in this Part II.D. are the most comprehensive and relevant references governing mDLs today. TSA also acknowledges that many additional standards and guidelines are in development covering diverse types of digital identification that can be issued and verified by different entities, both government and commercial. These emerging documents are expected to

[52] *See* comments submitted by Muller and UL.

concisely synthesize the large body of existing work from NIST and standards-development organizations, and will provide standardized mechanisms for mDLs. After carefully evaluating comments concerning emerging industry standards and closely observing ongoing development, TSA does not endorse any emerging standards at this time. TSA will continue to monitor development, and the future Phase 2 rulemaking may incorporate by reference pertinent parts of emerging standards (pending review of final published documents) that TSA believes are appropriate for Federal acceptance of mDLs for REAL ID official purposes.

E. DHS and TSA Involvement in mDLs

DHS and TSA have been actively participating in the mDL and digital identity space for many years to keep pace with industry developments. DHS has been participating in industry standards-development activities by serving as a non-voting member on working groups of the ISO/IEC and the W3C that are developing mDL/digital identity standards and technical specifications. Concurrently, DHS and TSA have been collaborating with industry to test the use of mDLs at various TSA security checkpoints. In 2022, TSA, under its collaboration with Apple (see Part II.C.3., above), launched a limited initiative that enables Arizona, Maryland, and Colorado residents to test the use of mDLs provisioned into the Apple Wallet app at select airport security checkpoints.[53] On May 18, 2023, TSA announced acceptance of Georgia mDLs provisioned into the Apple Wallet app at select airport security checkpoints.[54] Similarly, on March 1, 2023 and June 1, 2023, TSA announced acceptance of Utah-issued mDLs provisioned into the

---

[53] See TSA Biometrics Technology website, https://www.tsa.gov/biometrics-technology; Press Release, TSA, *TSA enables Arizona residents to use mobile driver's license or state ID for verification at Phoenix Sky Harbor International Airport* (Mar. 23, 2022), available at https://www.tsa.gov/news/press/releases/2022/03/23/tsa-enables-arizona-residents-use-mobile-drivers-license-or-state-id; Press Release, TSA, *TSA enables Maryland residents to use mobile driver's license or state ID for verification at Baltimore/Washington International and Reagan National Airports* (May 25, 2022), available at https://www.tsa.gov/news/press/releases/2022/05/25/tsa-enables-maryland-residents-use-mobile-drivers-license-or-state.

[54] Press release, TSA, *TSA enables Georgia residents to use mobile driver's license or state ID for verification at ATL* (May 18, 2023), available at https://www.tsa.gov/news/press/releases/2023/05/18/tsa-enables-georgia-residents-use-mobile-drivers-license-or-state-id

GET Mobile ID app, and Maryland-issued mDLs provisioned into the Google Wallet app, respectively, at select airports.[55] Utah utilizes a third-party mDL app produced by GET Group North America. DHS and TSA anticipate additional collaborations with other States and vendors in the future. These programs enable States, industry, and the Federal government to evaluate mDLs and ensure that they provide the security, privacy, and interoperability necessary for future, full-scale acceptance at Federal agencies for official purposes as defined in the REAL ID Act.

III. Summary of the Proposed Rule

A. Overview

In addition to revising definitions applicable to the REAL ID Act to incorporate mDLs, this rule proposes changes to 6 CFR part 37 that would enable TSA to grant a temporary waiver to States that TSA determines issue mDLs consistent with specified TSA requirements concerning security, privacy, and interoperability. This rule would enable Federal agencies, at their discretion, to accept for REAL ID official purposes, mDLs issued by a State that has been granted a waiver. The proposed rule would apply only to Federal agency acceptance of State-issued mDLs as defined in this proposed rule for REAL ID official purposes, but not other forms of digital identification, physical driver's licenses or physical identification cards, or non-REAL ID purposes. Any temporary waiver issued by TSA would be valid for a period of 3 years from the date of issuance. The waiver enabled by this rulemaking would be repealed when TSA publishes a Phase 2 rule that would set forth comprehensive requirements for mDLs.

---

[55] Press Release, TSA, *TSA using state-of-the art identity verification technology, accepting mobile driver licenses at SLC security checkpoint (Mar. 9, 2023), available at* https://www.tsa.gov/news/press/releases/2023/03/09/tsa-using-state-art-identity-verification-technology-accepting; Press Release, *TSA, TSA now accepts mobile IDs in Google Wallet on Android mobile devices, starting with the State of Maryland* (June 1, 2023), available at https://www.tsa.gov/news/press/releases/2023/06/01/tsa-now-accepts-mobile-ids-google-wallet-android-mobile-devices.

To obtain a waiver, a State would be required to submit an application, supporting data, and other documentation to establish that their mDLs meet TSA-specified criteria (discussed in Part III.B.4., below) concerning security, privacy, and interoperability. If the Secretary determines, upon evaluation of a State's application and supporting documents, that a State's mDL could be securely accepted under the terms of a waiver, the Secretary may issue such State a certificate of waiver. TSA intends to work with each State applying for a waiver on a case-by-case basis to ensure that its mDLs meet the minimum requirements necessary to obtain a waiver. This rulemaking would establish the full process for a State to apply for a waiver, including instructions for submitting the application and responding to subsequent communications from TSA as necessary, specific information and documents that a State must provide with its application, and requirements concerning timing, issuance of decisions, requests for reconsideration, and terms, conditions, and limitations related to waivers. To assist States that are considering applying for a waiver, TSA has developed guidelines, entitled, "Mobile Driver's License Waiver Application Guidance," which provide non-binding recommendations of some ways that States can meet the application requirements set forth in this rulemaking.[56]

TSA cautions, however, that the waiver enabled by this rulemaking is not a commitment by Federal agencies to accept mDLs issued by a State to whom TSA has granted a waiver. Federal agencies exercise full discretion over their identity verification policies, which may be subject to change. A Federal agency that accepts mDLs may suddenly halt acceptance for reasons beyond the agency's control, such as suspension or

[56] The specific measures and practices discussed in the DHS Waiver Application Guidance are neither mandatory nor necessarily the "preferred solution" for complying with the requirements proposed in the rule. Rather, they are examples of measures and practices that a State issuer of mDLs may choose to consider as part of its overall strategy to issue mDLs. States have the ability to choose and implement other measures to meet these requirements based on factors appropriate to that State, so long as DHS determines that the measures implemented provide the levels of security and data integrity necessary for Federal acceptance of mDLs for official purposes as defined in the REAL ID Act and 6 CFR part 37. As provided in proposed § 37.10(c) of 6 CFR part 37, DHS may periodically update the Guidance as necessary to recommend mitigations of evolving threats to security, privacy, or data integrity.

termination of a waiver, technical issues with IT systems, or a loss of resources to support mDLs. In such instances, an mDL holder seeking to use an mDL for REAL ID official purposes (including boarding commercially regulated aircraft or access to Federal facilities) may be denied such uses. To avoid this issue, TSA strongly urges all mDL holders to carry their physical REAL ID cards in addition to their mDLs. This will ensure that mDL holders are not disenfranchised from REAL ID uses if a Federal agency does not accept mDLs. Indeed, TSA has long advised that passengers who choose to present mDLs in TSA checkpoint testing must continue to have their physical cards readily available in the event that a TSA officer requires such identification.[57] TSA also recommends to Federal agencies that they regularly inform the public, in a form and manner of their choosing, of their mDL acceptance policies. TSA urges the public to view mDLs not as a replacement of physical REAL ID cards, but as a complement to them.

B. Specific Provisions

1. Definitions

TSA proposes adding new definitions to subpart A, § 37.3. In particular, new definitions for "mobile driver's license" and "mobile identification card" are necessary because the current regulations predated the emergence of mDL technology and, therefore, does not define these terms. Additionally, the definitions reflect changes made by the REAL ID Modernization Act, which amended the definitions of "driver's license" and "identification card" to specifically include "mobile or digital driver's licenses" and "mobile or digital identification cards." The proposed definitions in this rule would provide a more precise definition of "mobile driver's license" and "mobile identification card" by clarifying that those forms of identification require a mobile electronic device to store the identification information, as well as an electronic device to read that

[57] *See, e.g.,* https://www.tsa.gov/real-id (see FAQ for "Does TSA accept mobile driver's licenses?").

information. TSA also proposes adding a new definition of "mDL" that collectively refers to mobile versions of both State-issued driver's licenses and State-issued identification cards as defined in the REAL ID Act. TSA also proposes adding additional definitions to explain terms used in § 37.10(a) and appendix A to subpart A to the part. For example, the proposed rule would add new defintions for "digital certificates" and "certificate systems," which are necessary elements of risk controls for the IT systems that States use to issue mDLs. In addition, the rulemaking proposes adding a definition for "certificate policy," which forms the governance framework for the State's certificate systems. A State must develop, maintain, and execute a certificate policy to comply with the requirements set forth in appendix A to subpart A of the part.

2. TSA Issuance of Temporary Waiver from § 37.5(b) and State Eligibility Criteria

TSA proposes adding to subpart A new § 37.7, entitled "Temporary waiver for mDLs; State eligibility," to establish the availability of a temporary waiver for a State to exempt its mDLs from meeting the card-based compliance requirement of § 37.5(b). Section 37.7(a) authorizes TSA to issue a temporary certificate of waiver to States that submit an application for a waiver that demonstrates compliance with application criteria set forth in § 37.10(a) and (b). This waiver would only apply to mDLs, not physical cards, and would not waive the requirement in § 37.5(b) regarding State-based compliance or any other requirements in the regulations. Issuance of a certificate of waiver to a State would permit Federal agencies to continue accepting for official purposes mDLs issued by those States when REAL ID enforcement begins on May 7, 2025. The mere issuance of a waiver to a State, however, does not obligate any Federal agency to accept an mDL issued by such State; each Federal agency retains discretion to determine its own policies regarding identification, including whether to accept mDLs.

To be eligible for consideration for a waiver, a State must meet the criteria set forth in proposed § 37.7(b). These criteria require that the issuing State: is in full compliance with REAL ID requirements; has submitted an application demonstrating that the State issues mDLs that provide security, privacy, and interoperability necessary for Federal acceptance; and issues mDLs only to individuals who have been issued a valid and unexpired REAL ID-compliant physical driver's license or identification card. TSA's determination of whether a State satisfies the eligibility criteria would be based on TSA's evaluation of the information provided by the State in its application (see Part III.B.4., below), as well as other information available to TSA.

3. Requirements for Federal Agencies that Accept mDLs

TSA proposes adding to subpart A new § 37.8, entitled "Requirements for Federal agencies accepting mDLs issued by States with temporary waiver." This section proposes that any Federal agency that elects to accept mDLs for REAL ID official purposes must meet three requirements in proposed new § 37.8. First, a Federal agency must confirm that the State holds a valid certificate of waiver. Agencies would make this confirmation by verifying that the State's name appears in a list of States to whom TSA has granted a waiver. TSA would publish this list on the REAL ID website at www.dhs.gov/real-id/mDL (as provided in § 37.9(b)(1)). Second, Federal agencies must use an mDL reader to retrieve mDL data from an individual's mobile device, and validate that the data is authentic and unchanged. To retrieve and validate mDL data, Federal agencies must follow the processes required by industry standard ISO/IEC 18013-5:2021. Finally, if a State discovers that acceptance of a State's mDL is likely to cause imminent or serious threats to the security, privacy, or data integrity, the State must notify TSA at www.dhs.gov/real-id/mDL within 72 hours of such discovery. Examples of such triggering events include cyber-attacks and other events that cause serious harm to a State's mDL issuance system. TSA would consider whether such information warrants

suspension of that State's waiver under § 37.9(e)(4)(i)(B) (see discussion in Part III.B.6., below). If TSA elects not to issue a suspension, Federal agencies would continue to exercise their own discretion regarding continuing acceptance of mDLs.

4. Requirements for States Seeking to Apply for a Waiver

TSA proposes adding to subpart A new § 37.9, which would set forth a process for a State to request a temporary certificate of waiver established in new § 37.7. As provided in § 37.9(a), a State seeking a waiver must file a complete application as set forth in § 37.10(a) and (b), following instructions that would be available at www.dhs.gov/real-id/mDL. Section 37.10(a) and (b) would set forth all information, documents, and data that a State must include in its application for a waiver. TSA is proposing that if TSA determines that the means that a State implements to comply with the requirements in § 37.10(a) and (b) provide the requisite levels of security, privacy, and data integrity for Federal acceptance of mDLs for official purposes, TSA would grant such State a waiver. TSA does not, however, propose prescribing specific means (other than the requirements specified in appendix A to subpart A of the part, which is discussed further in Part III.B.4.iv, below) that a State must implement. Instead, States would retain broad discretion to choose and implement measures to meet these requirements based on factors appropriate to that State.

(i) Application Requirements

As set forth in § 37.10(a)(1) through (4), a State would be required to establish in its application how it issues mDL under the specified criteria for security, privacy, and interoperability suitable for acceptance by Federal agencies, as follows:

- Paragraph (a)(1) would set forth requirements for mDL provisioning.
- Paragraph (a)(2) would specify requirements for managing State Certificate Systems, which are set forth in appendix A to subpart A of the part.

- Paragraph (a)(3) would require a State to demonstrate how it protects personally identifiable information of individuals during the mDL provisioning process.
- Paragraph (a)(4) would require a State to establish: how it issues mDLs that are interoperable with requirements set forth in standard ISO/IEC 18013-5:2021; that the State uses only those algorithms for encryption,[58] secure hash function,[59] and digital signatures that are specified in ISO/IEC 18013-5:2021, and in NIST FIPS PUB 180-4, 186-5, 197, 198-1, and 202; and how the State complies with the "AAMVA mDL data element set" as defined in the AAMVA mDL Guidelines v. 1.2, Section 3.2 (see Part II.D., above, for a detailed discussion of those references).

(ii) Audit Requirements

Section 37.10(b) would require a State to submit an audit report prepared by an independent auditor verifying the accuracy of the information provided by the State in response to § 37.10(a), as follows:

- Paragraph (1) would set forth specific experience, qualifications, and accreditations that an auditor must meet.
- Paragraph (2) would require a State to provide information demonstrating the absence of a potential conflict of interest of the auditing entity.

(iii) Waiver Application Guidance

As set forth in § 37.10(c), TSA proposes to publish "Mobile Driver's License Waiver Application Guidance," in the *Federal Register* and on the REAL ID website at

---

[58] Encryption refers to the process of cryptographically transforming data into a form in a manner that conceals the data's original meaning to prevent it from being read. Decryption is the process of restoring encrypted data to its original state. [IETF RFC 4949, *Internet Security Glossary, Version 2*, August 2007]

[59] A function that processes an input value creating a fixed-length output value using a method that is not reversible (i.e. given the output value of a function it is computationally impractical to find the function's corresponding input value).

www.dhs.gov/real-id/mDL to assist States in completing their applications. The proposed guidance document is available for review at www.regulations.gov/docket/TSA-2023-0002. TSA is accepting comments on the guidance along with this proposed rule. This guidance would provide TSA's recommendations for some ways that States can meet the requirements in § 37.10(a)(1). The guidance would *not* establish legally enforceable requirements for a States applying for a waiver. Instead, the guidance would provide non-binding examples of measures and practices that a State may choose to consider as part of its overall strategy to issue mDLs. States continue to exercise discretion to select processes not included in the Guidance. Given the rapidly-evolving cyber threat landscape, however, TSA may periodically update its guidance to provide additional information regarding newly-published standards or other sources, or recommend mitigations of newly discovered risks to the mDL ecosystem. TSA would publish updated guidance in the *Federal Register* and on the REAL ID website at www.dhs.gov/real-id/mDL, and would provide a copy to all States that have applied for or been issued a certificate of waiver. Updates to guidance will not impact issued waivers or pending applications.

(iv) Appendix A to Subpart A: Requirements for State mDL Issuance Systems

Appendix A to subpart A of the part sets forth fundamental requirements to ensure the security and integrity of State mDL issuance processes. More specifically, these requirements concern the creation, issuance, use, revocation, and destruction of the State's certificate systems and cryptographic keys. The appendix consists of requirements in eight categories: (1) Certificate Authority Certificate Life Cycle Policy, (2) Certificate Authority Access Management, (3) Facility, Management, and Operational Controls, (4) Personnel Security Controls, (5) Technical Security Controls, (6) Threat Detection, (7) Logging, and (8) Incident Response and Recovery Plan. Adherence to

these requirements ensures that States issue mDLs in a standardized manner with security and integrity to establish the trust necessary for Federal acceptance for official purposes.

- Certificate Authority Certificate Life Cycle Policy requirements (appendix A, sec. 1) ensure that a State issuing an mDL creates and manages a formal process which follows standardized management and protections of digital certificates. These requirements must be implemented in full compliance with the references cited in the appendix: the CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA Browser Forum Network and Certificate System Security Requirement, NIST Cybersecurity Framework, NIST SP 800-53 Rev. 5, NIST SP 800-57, and NIST SP 800-53B.
- Certificate Authority Access Management requirements (appendix A, sec. 2) set forth policies and processes for States concerning, for example, restricting access to mDL issuance systems, policies for multi-factor authentication, defining the scope and role of personnel, and Certificate System architecture which separates and isolates Certificate System functions to defined security zones. These requirements must be implemented in full compliance with the references cited in the appendix: CA Browser Forum Network and Certificate System Security Requirements, NIST Cybersecurity Framework, NIST 800-53 Rev. 5, NIST SP 800-63-3, and NIST SP 800-63B.
- Under the requirements concerning Facility, Management, and Operational Controls (appendix A, sec. 3), States must provide specified controls protecting facilities where Certificate Systems reside from unauthorized access, environmental damage, physical breaches, and risks from foreign ownership, control, or influence. These requirements must be implemented in full compliance with the references cited in the appendix: NIST SP 800-53 Rev. 5.

- Personnel security controls (appendix A, sec. 4) require States to establish policies to control insider threat risks to Certificate Systems and facilities. Such policies must include establish screening criteria for personnel who access Certificate Systems, post-employment access termination, updates to personnel security policy, training, records retention schedules, among other policies. These requirements must be implemented in full compliance with the references cited in the appendix: NIST SP 800-53 Rev. 5 and CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
- Technical security controls (appendix A, sec. 5) specify requirements to protect Certificate System networks. In addition, States are required to protect private cryptographic keys of Issuing Authority Root Certificates using hardware security modules of Level 3 or higher and Document Signer private cryptographic keys in hardware security modules of Level 2 and higher. Other controls are specified regarding Certificate System architecture and cryptographic key generation processes. These requirements must be implemented in full compliance with the references cited in the appendix: CA Browser Forum Network and Certificate System Security Requirements, CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, NIST Cybersecurity Framework, NIST SP 800-53 Rev. 5, NIST SP 800-57, and NIST FIPS 140-3.
- Under requirements for threat detection (appendix A, sec. 6), States must implement controls to monitor and log evolving threats to various mDL issuance infrastructure, including digital certificate, issuance, and support systems. These requirements must be implemented in full compliance with the references cited in the appendix: CA Browser Forum Network and Certificate System Security

Requirements, CISA Cybersecurity Incident & Vulnerability Response Playbooks, NIST Cybersecurity Framework, NIST SP 800-53 Rev. 5.

- Logging controls (appendix A, sec. 7) require States to record various events concerning Certificate Systems, including the management of cryptographic keys, digital certificate lifecycle events. The controls set forth detailed requirements concerning specific types of events that must be logged, as well as timeframes for maintaining such logs. These requirements must be implemented in full compliance with the references cited in the appendix: CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, NIST Cybersecurity Framework, and NIST SP 800-53 Rev. 5.
- Finally, section 8 of appendix A requires States to implement policies to respond to and recover from security incidents. States must act on logged events, issue alerts to relevant personnel, respond to alerts within a specified time period, perform vulnerability scans, among other things. In particular, States must provide written notice to TSA at www.dhs.gov/real-id/mDL within 72 hours of discovery of a significant cyber incident or breach that could compromise the integrity of a Certificate System. These requirements must be implemented in full compliance with the references cited in the appendix: CA Browser Forum Network and Certificate System Security Requirements, CISA Cybersecurity Incident & Vulnerability Response Playbooks, CISA National Cyber Incident Response Plan; NIST SP 800-53 Rev. 5, NIST Cybersecurity Framework.

TSA invites comment on all aspects of the waiver application requirements and costs of compliance, including the Waiver Application Guidance, appendix A to subpart A to the part, the appropriateness of requiring compliance with the specified standards and guidelines and any alternate standards that should be considered, and other recommendations that commenters believe TSA should consider.

5. Decisions on Applications for Waiver

Section 37.9(b) would establish a timeline and process for TSA to issue decisions on a waiver application. Under this paragraph, TSA would endeavor to provide States a decision on initial applications within 60 days, but not longer than 90 days. TSA would provide three types of written notice via email: approved, insufficient, or denied.

If TSA approves a State's application for a waiver, TSA would memorialize that decision by issuing a certificate of waiver to that State, and including the State in a list of State-mDLs approved for Federal use, published by TSA on the REAL ID website at www.dhs.gov/real-id/mDL. A certificate of waiver would specify the date that the waiver becomes effective, the expiration date, and any other terms and conditions with which a State must comply, as provided under proposed § 37.9(d). A State seeking to renew its certificate beyond the expiration date must reapply for a waiver, as provided in § 37.9(e)(6).

If TSA determines that an application is insufficient, did not respond to certain information required in § 37.10(a) or (b), or contains other deficiencies, TSA would provide an explanation of such deficiencies and allow the State an opportunity address the deficiencies within the timeframe specified in § 37.9(b)(2). TSA would permit States to submit multiple amended applications if necessary, with the intent of working with States individually to enable their mDLs to comply with the requirements of § 37.10(a) and (b).

If TSA denies an application, TSA would provide the specific grounds for the basis of the denial and afford the State an opportunity to submit a new application. As stated in § 37.9(c), TSA would also provide a State an opportunity to seek reconsideration of a denied application. Instructions for seeking reconsideration would be provided by TSA on the REAL ID website at www.dhs.gov/real-id/mDL. An adverse decision upon reconsideration would be considered a final agency action. As provided in

§ 37.9(c), however, a State whose request for reconsideration has been denied may submit a new application for a waiver.

6. Limitations, Suspension, and Termination of Certificate of Waiver

Section 37.9(e) would set forth various restrictions on a certificate of waiver. Specifically, in paragraph (e)(1) of this section, TSA proposes that a certificate of waiver would be valid for a period of three years from the date of issuance. Paragraph (e)(2) proposes that a State must report to TSA if, after it receives a waiver, it makes significant modifications to its mDL issuance processes that differ in a material way from information that the State provided in its application. If the State makes such modifications, it would be required to report such changes 60 days before implementing the changes. This requirement is intended to apply to changes that may undermine the bases on which TSA granted a waiver. The reporting requirement is not intended to apply to routine, low-level changes, such as systems maintenance and software updates and patches. Paragraph (e)(3) would require a State that is issued a waiver to comply with all requirements specified in §§ 37.51(a) and 37.9(d)(3).

Section 37.9(e)(4) sets forth processes for suspension of certificates of waiver. As provided in proposed § 37.9(e)(4)(i)(A), TSA may suspend the validity of a certificate of waiver if TSA determines that a State:

- fails to comply with any terms and conditions (see § 37.9(d)(3)) specified in the certificate of waiver;
- fails to comply with reporting requirements (see § 37.9(e)(2)); or
- issues mDLs in a manner that is not consistent with the information the State provided in its application for a waiver under § 37.10(a) and (b).

Before suspending a waiver for these reasons, TSA will provide such State written notice via email that it intends to suspend its waiver, along with an explanation of the reasons, information on how the State may address the deficiencies, and a timeline for the State to

respond and for TSA to reply to the State, as set forth in § 37.9(e)(4)(ii). DHS may withdraw the notice of suspension, request additional information, or issue a final suspension. If TSA issues a final suspension of a State's certificate of waiver, DHS will remove the name of that State from the list of mDLs approved for Federal acceptance for official purposes.

TSA additionally may suspend a State's waiver at any time upon discovery that Federal acceptance of a State's mDL is likely to cause imminent or serious threats to the security, privacy, or data integrity of any Federal agency, as proposed by § 37.9(e)(4)(i)(B). Suspension would apply to all Federal agencies and would not be agency-specific. Examples of such triggering events include cyber-attacks and other events that cause serious harm to a State's mDL issuance systems. If a State discovers a significant cyber incident that it believes could compromise the integrity of its mDL issuance systems, sec. 8.6 of appendix A to subpart A of the part would require States to provide written notice to TSA, at www.dhs.gov/real-id/mDL, of such incident within 72 hours of discovery. If TSA determines such suspension is necessary, TSA will provide written notice via email to each State whose certificate of waiver is affected, as soon as practicable after discovery of the triggering event, providing an explanation for the suspension, as well as an estimated timeframe for resumption of the validity of the certificate of waiver.

It is TSA's intent to work with States to resolve the conditions that could lead to suspension and avoid issuing a final suspension. If TSA issues a final suspension of any State's certificate of waiver, TSA will temporarily remove the name of that State from the list of mDLs approved for Federal acceptance for official purposes. A State receiving a final suspension may apply for a new certificate of waiver by submitting a new application. Under § 37.9(e)(5), TSA may terminate a certificate of waiver for serious or

egregious violations. More specifically, TSA may terminate a waiver if TSA determines that a State:

- does not comply with REAL ID requirements in § 37.51(a);
- is committing an egregious violation of any terms and conditions (see § 37.9(d)(3)) specified in the certificate of waiver and is unwilling to cure such violation;
- is committing an egregious violation of reporting requirements (see § 37.9(e)(2)) and is unwilling to cure such violation; or
- provided false information in its waiver application.

Before terminating a certificate of waiver, TSA would provide written notice via email of intent to terminate, including findings supporting the termination and an opportunity to present information. As specified, a State would have 7 days to respond to the notice, and TSA would respond via email within 30 days. TSA may withdraw the notice of termination, request additional information, or issue a final termination. If TSA issues a final termination of a State's certificate of waiver, TSA will remove the name of that State from the list of mDLs approved for Federal acceptance for official purposes. A State whose certificate of waiver has been terminated may apply for a new certificate of waiver by submitting a new application.

7. Effect of a Status of Waiver on REAL ID Compliance

Section 37.9(f) clarifies that the status of a State's certificate of waiver, including the status of an application for a waiver, has no bearing on TSA's determination of that State's compliance or non-compliance with any other section of this part. A certificate of waiver that TSA has issued to a State is not a determination that the State is in compliance with any other section in this part. Similarly, an application for a waiver that TSA has deemed insufficient or denied, or a certificate of waiver TSA has suspended,

terminated, or expired, is not a determination that the State is not in compliance with any other section in this part.

8. Incorporation by Reference

TSA proposes adding to subpart A, § 37.4, the following industry standards and government guidelines that this rulemaking proposes to incorporate by reference (discussed in detail in Part II.D., above):

- AAMVA
    - Mobile Driver's License (mDL) Implementation Guidelines, Version 1.2 (Jan. 2023);
- CA/Browser Forum
    - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 1.8.6 (Dec. 14, 2022),
    - Network and Certificate System Security Requirements, Version 1.7 (Apr. 5, 2021);
- CISA
    - Cybersecurity Incident & Vulnerability Response Playbooks (Nov. 2021),
    - National Cyber Incident Response Plan (Dec. 2016);
- ISO/IEC
    - ISO/IEC 18013-5:2021, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application, Edition 1 (Sept. 2021);
- NIST
    - FIPS PUB 140-3, Security Requirements for Cryptographic Modules (Mar. 22, 2019),
    - FIPS PUB 180-4, Secure Hash Standard (SHS) (Aug. 2015),

- FIPS PUB 186-5, Digital Signature Standard (DSS) (Feb. 2023),
- FIPS PUB 197, Advanced Encryption Standard (AES) (Nov. 26, 2001),
- FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC) (July 2008),
- FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (Aug. 2015),
- SP 800-53, Security and Privacy Controls for Information Systems and Organizations, Rev. 5 (Sept. 2020),
- SP 800-57 Part 1, Recommendation for Key Management: Part 1 – General, Rev. 5 (May 2020),
- SP 800-57 Part 2, Recommendation for Key Management: Part 2 – Best Practices for Key Management Organization, Rev. 1 (May 2019),
- SP 800-57 Part 3, Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance, Rev. 1 (Jan. 2015),
- SP 800-63-3, Digital Identity Guidelines, (June 2017),
- SP 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management (June 2017), and
- Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Apr. 16, 2018).

C. Impacted Stakeholders

The proposed changes would apply to State driver's licensing agencies issuing mDLs that seek a temporary waiver from TSA for its mDLs. The waiver would enable Federal agencies to accept such mDLs for official purposes, defined in the REAL ID Act

as accessing Federal facilities, entering nuclear power plants, boarding federally regulated commercial aircraft, and any other purposes that the Secretary shall determine. Any Federal agency that chooses to accept mDLs for official purposes must procure a reader in order to receive an individual's identity data.

This proposed rule does not impose any requirements on:

- States that do not seek a waiver for mDLs;
- Non-State issuers of other forms of digital identification; or
- Federal agencies to accept mDLs.

A State seeking a waiver for Federal acceptance of its mDLs for official purposes would be required to file with TSA a complete application and supporting documents. An application form and instructions would be published by TSA in a form and manner prescribed by TSA, such as a TSA-specified website. Through the application, the State would be required to demonstrate how its mDLs meet the requirements for a waiver set forth in § 37.10(a) and (b).

D. Use Cases Affected by this Proposed Rule

The scope of this proposed rule is confined strictly to Federal acceptance of mDLs for official purposes, defined by the REAL ID regulations as accessing Federal facilities, entering nuclear power plants, and boarding federally regulated commercial aircraft. Any other purpose is beyond the scope of this rulemaking. For example, a waiver issued under this proposed rule would not apply to any of the following:

- mDL acceptance by Federal agencies for non-REAL ID official uses (*e.g.,* applying for Federal benefits);
- mDL acceptance by non-Federal agencies (*e.g.,* State agencies, businesses, private persons);
- Commercial transactions; or
- Physical driver's licenses or identification cards.

Nothing in this proposed rule would *require* Federal agencies to accept mDLs; each Federal agency retains the discretion to determine its identification policies. Additionally, nothing in this proposed rule would require a State to seek a waiver or issue mDLs.

IV. Discussion of Public Comments in the RFI

As discussed in Part II.B., above, DHS issued an RFI[60] on April 19, 2021, and requested comments from the public to be submitted by June 18, 2021. In addition, DHS and TSA held a virtual public meeting on June 30, 2021, to provide an additional forum for public comments, and extended the RFI comment period until July 30, 2021, to permit additional comments following the public meeting. [61] Approximately 100 persons attended the public meeting. In response to discussion at the public meeting and comments to the RFI concerning the importance of access to the primary industry standard referenced in the RFI, ISO/IEC 18013-5:2021, DHS facilitated public access to the standard by publishing a notification[62] in the *Federal Register* on September 16, 2021, providing instructions to the public to gain access to the standard without cost. Approximately 30 persons requested and received access. Additionally, DHS reopened the comment period until October 18, 2021. With the comment period extension and reopening, DHS provided a total RFI comment period of 180 days.

DHS received roughly 60 comments to the RFI from a diverse group of stakeholders, including advocacy groups representing varied interests, individuals, State government agencies, trade associations, and industry. An analysis of comments received showed that topics of interest to stakeholders concerned: the

[60] 86 FR 20320.
[61] 86 FR 31987.
[62] 86 FR 51625.

need for standardization and/or Federal guidance,[63] potential benefits to the public from mDLs generally,[64] and the appropriateness of ISO/IEC standards as a starting point for regulatory requirements.[65] Input received from these stakeholders, as it relates to the focus of this NPRM, is included and referenced throughout this proposed rule.

In addition to the issues already discussed, many commenters raised concerns about potential privacy risks depending on the mode of data transfer. For background, an mDL reader can retrieve an individual's data under two different modes of operation: a "device retrieval" mode (also known as "offline") in which data is retrieved directly from an mDL holder's mobile device, and a "server retrieval" mode (also known as "online") in which the data is retrieved from a State driver's licensing agency.[66] In its RFI, DHS noted that it was considering both modes of operation for Federal acceptance for official purposes, and specifically sought comments on the security and privacy risks, and mitigating solutions for both modes.[67] DHS received numerous comments from advocacy groups, industry, and States concerning potential privacy risks posed specifically by server retrieval mode.[68] Chief among these concerns was the potential for mDL usage to be tracked. TSA has observed that security and privacy protections to

---

[63] *See, e.g.*, comments submitted by: American Association of Motor Vehicles Administrators; CBN Secure Technologies; DocuSign; FaceTec; IDmachines; Maryland DHS of Transportation, Motor Vehicle Administration; National Conference of State Legislatures; State of Connecticut, DHS of Motor Vehicles; U.S. Travel Association.

[64] *See, e.g.*, comments submitted by: Applied Recognition; Bredemarket; Hiday; IDmachines; Mothershed; Muller; State of Connecticut, DHS of Motor Vehicles; U.S. Travel Association.

[65] *See, e.g.*, comments submitted by: American Association of Motor Vehicle Administrators; American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center; Apple; Association for Convenience & Fuel Retailing; CBN Secure Technologies; FaceTec; Florida DHS of Highway Safety and Motor Vehicles; IDEMIA; Maryland DHS of Transportation, Motor Vehicle Administration; National Immigration Law Center and Undersigned Organizations; Secure Technology Alliance; State of Connecticut, DHS of Motor Vehicles; Underwriters Laboratories; Verifiable Credentials Policy Committee, Blockchain Advocacy Coalition.

[66] 86 FR 20323-24.

[67] 86 FR 20326.

[68] *See, e.g.*, comments submitted by American Association of Motor Vehicle Administrators; American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center; Association for Convenience and Fuel Retailing; Better Identity Coalition; Electronic Privacy Information Center; IDEMIA; National Immigration Law Center, and Undersigned Organizations; and Verifiable Credentials Policy Committee - Blockchain Advocacy Coalition.

mitigate such concerns are evolving and unsettled, and after careful consideration of commenters' concerns, TSA does not believe server retrieval mode is appropriate for Federal acceptance for official purposes at this time. TSA will continue monitoring industry developments and may update its conclusions in the Phase 2 rulemaking, if warranted.

DHS also received comments on other topics, including non-REAL ID use cases such as commercial transactions and technical information on various topics. As noted above, a waiver issued under the proposed rule would not address use of an mDL for commercial transactions or any other non-Federal purposes not covered by the REAL ID Act or regulations. In general, mDL acceptance by Federal agencies for non-REAL ID official purposes, mDL acceptance by non-Federal agencies, and mDL use in commercial transactions go beyond the scope of the REAL ID Act's official purposes. Although not the focus of this proposal, TSA may examine some of these issues through its on-going mDL efforts, such as mDL collaborations with industry, which could inform future regulatory proposals. To support this interest, TSA appreciates stakeholders' perspectives on these topics.

V. Consultation with States, Non-Governmental Organizations, and the Department of Transportation

Under section 205 of the REAL ID Act, issuance of REAL ID regulations must be conducted in consultation with the Secretary of Transportation and the States. During the development of this NPRM, DHS and TSA consulted with the Department of Transportation and other Federal agencies with an interest in this rulemaking. DHS and TSA also consulted with State officials via AAMVA. In addition, DHS and TSA met with various non-governmental organizations, including civil rights and privacy advocacy groups. Stakeholder input, informed by extensive outreach, was critical to informing this NPRM.

VI. Regulatory Analyses

A. Economic Impact Analyses

1. Regulatory Impact Analysis Summary

Changes to Federal regulations must undergo several economic analyses. First, E.O. 12866 of September 30, 1993 (Regulatory Planning and Review),[69] as supplemented by E.O. 13563 of January 18, 2011 (Improving Regulation and Regulatory Review),[70] and amended by E.O. 14094 of April 6, 2023 (Modernizing Regulatory Review)[71] directs Federal agencies to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (RFA)[72] requires agencies to consider the economic impact of regulatory changes on small entities. Third, the Trade Agreement Act of 1979[73] prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995[74] (UMRA) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted for inflation) in any one year.

2. Assessments Required by E.O. 12866 and E.O. 13563

E.O. 12866 and E.O. 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Under E.O. 12866, as

---

[69] Published at 58 FR 51735 (Oct. 4, 1993).
[70] Published at 76 FR 3821 (Jan. 21, 2011).
[71] Published at 88 FR 21879 (April 6, 2023).
[72] Public Law 96-354, 94 Stat. 1164 (Sept. 19, 1980) (codified at 5 U.S.C. 601 *et seq*., as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA)).
[73] Public Law 96–39, 93 Stat. 144 (July 26, 1979) (codified at 19 U.S.C. 2531-2533).
[74] Public Law 104-4, 109 Stat. 66 (Mar. 22, 1995) (codified at 2 U.S.C. 1181-1538).

amended by E.O. 14094, agencies must also determine whether a regulatory action is significant.[75] These requirements were supplemented by E.O. 13563, which emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility.

In conducting these analyses, TSA has made the following determinations:

(a) While TSA attempts to quantify costs where available, TSA primarily discusses the costs and benefits of this rulemaking in qualitative terms. At present, mDLs are part of an emerging and evolving industry with an elevated level of uncertainty surrounding costs and benefits. Nonetheless, TSA anticipates the rulemaking would not result in an effect on the economy of $200 million or more in any year of the analysis. The rulemaking would not adversely affect the economy, interfere with actions taken or planned by other agencies, or generally alter the budgetary impact of any entitlements.

(b) TSA has not prepared an Initial Regulatory Flexibility Analysis (IRFA) and, pursuant to 5 U.S.C. 605(b), the Secretary certifies that the proposed rule would not have a significant economic impact on a substantial number of small entities. The proposed rule would only directly regulate the fifty States, the District of Columbia, and the five U.S. territories who voluntarily participate in the mDL waiver process, who under the RFA are not considered small entities.

(c) TSA has determined that the NPRM imposes no significant barriers to international trade as defined by the Trade Agreement Act of 1979; and

---

[75] See section 1(b) of E.O. 14094, revising section 3(f) of E.O. 12866. Section 3(f) of EO 12866 defines a "significant regulatory action" as any regulatory action that is likely to result in a rule that: (1) has an annual effect on the economy of $200 million or more or adversely affects in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, territorial, or tribal governments or communities (also referred to as economically significant); (2) creates serious inconsistency or otherwise interferes with an action taken or planned by another agency; (3) materially alters the budgetary impacts of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raises novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the EO.

(d) TSA has determined that the NPRM does not impose an unfunded mandate on State, local, or tribal governments, such that a written statement would be required under the UMRA, as its annual effect on the economy does not exceed the $100 million threshold (adjusted for inflation) in any year of the analysis.

TSA has prepared an analysis of its estimated costs and benefits, summarized in the following paragraphs, and in the OMB Circular A-4 Accounting Statement. When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. For this proposed rule's period of analysis, TSA uses a 10-year period of analysis to estimate costs.

This proposed rule would establish a temporary waiver process that would permit Federal agencies to accept mDLs for official purposes, as defined in the REAL ID Act, when full enforcement of the REAL ID Act and regulations begins on May 7, 2025. Federal agencies would be able to accept mDLs for official purposes on an interim basis, provided that: (1) the mDL holder has been issued a valid and unexpired REAL ID-compliant physical driver's license or identification card from the same State that issued the mDL; (2) TSA has determined the issuing State to be REAL ID-compliant; and (3) TSA has issued a waiver to the State. Federal agencies that opt to accept mDLs for official purposes must also procure a mDL reader in order to validate the identity of the mDL holder. As part of the application process for the mDL waiver, States would be required to submit to TSA an application, including supporting data, and other documentation necessary to establish that their mDLs meet specified criteria concerning security, privacy, and interoperability. The criteria concerning security, privacy, and interoperability would not change absent a subsequent rulemaking. When REAL ID Act and regulations enforcement begins on May 7, 2025, Federal agencies will be prohibited from accepting non-compliant driver's licenses and identification cards, including both physical cards and mDLs, for official purposes.

In the following paragraph TSA summarizes the estimated costs of the proposed rule on the affected parties: States, TSA, mDL users, and relying parties (Federal agencies that voluntarily choose to accept mDLs for official purposes). TSA has also identified other non-quantified impacts to affected parties. As Table 1 displays, TSA estimates the 10-year total cost of the proposed rule to be $826.8 million undiscounted, $695.6 million discounted at 3 percent, and $562.0 million discounted at 7 percent. The total cost to States comprises approximately 98 percent of the total quantified costs of the proposed rule.

Table 1: Total Cost of the Proposed Rule by Entity ($ Thousands)

Year	States Cost	TSA Cost	Relying Party Cost	Total Proposed Rule Cost		
				d = a + b + c		
	a	b	c	Undiscounted	Discounted at 3%	Discounted at 7%
1	$42,957	$1,589	$40	$44,586	$43,287	$41,669
2	$62,842	$1,662	$459	$64,963	$61,234	$56,741
3	$71,374	$1,174	$269	$72,818	$66,638	$59,441
4	$83,278	$1,069	$191	$84,538	$75,111	$64,494
5	$94,531	$833	$188	$95,551	$82,423	$68,127
6	$91,485	$669	$580	$92,734	$77,663	$61,793
7	$91,974	$702	$371	$93,047	$75,655	$57,945
8	$91,811	$703	$279	$92,793	$73,252	$54,007
9	$91,485	$691	$266	$92,442	$70,849	$50,283
10	$91,974	$746	$645	$93,364	$69,472	$47,462
Total	**$813,712**	**$9,839**	**$3,286**	**$826,837**	**$695,586**	**$561,960**
Annualized					**$81,544**	**$80,010**

Note: Totals may not add due to rounding.

States incur costs to familiarize themselves with the requirements of the proposed rule, purchase access to an industry standard, submit their mDL waiver application, submit an mDL waiver reapplication, and comply with mDL application criteria requirements. As displayed in Table 2, the 10-year cost to States is $813.7 million undiscounted, $684.2 million discounted at 3 percent, and $552.4 million discounted at 7 percent.

Table 2: Total Cost of the Proposed Rule to States ($ Thousands)

Year	Familiar-ization Cost	Stand-ards Cost	Waiver Applic-ation Cost	Reapplic-ation Cost	Esca-lated Review Cost	Infras-tructure Security Cost	Total Cost to States		
							g = a + b + c + d + e + f		
	a	b	c	d	e	f	Undis-counted	Disc-ounted at 3%	Disc-ounted at 7%
1	$63.3	$1.9	$675.0	$0	$4.6	$42,212	$42,957	$41,705	$40,146
2	$0	$1.3	$450.0	$0	$7.7	$62,383	$62,842	$59,234	$54,888
3	$0	$0.6	$225.0	$0	$9.2	$71,140	$71,374	$65,318	$58,263
4	$0	$0.6	$225.0	$488.5	$10.8	$82,553	$83,278	$73,992	$63,533
5	$0	$0.6	$225.0	$325.6	$12.3	$93,967	$94,531	$81,543	$67,399
6	$0	$0	$0	$162.8	$12.3	$91,310	$91,485	$76,618	$60,961
7	$0	$0	$0	$651.3	$12.3	$91,310	$91,974	$74,783	$57,277
8	$0	$0	$0	$488.5	$12.3	$91,310	$91,811	$72,477	$53,435
9	$0	$0	$0	$162.8	$12.3	$91,310	$91,485	$70,116	$49,762
10	$0	$0	$0	$651.3	$12.3	$91,310	$91,974	$68,437	$46,755
Total	**$63.3**	**$5.0**	**$1,800.0**	**$2,930.8**	**$106.0**	**$808,807**	**$813,712**	**$684,223**	**$552,419**
Annual-ized								**$80,212**	**$78,652**

Note: Totals may not add due to rounding.

TSA incurs costs associated with reviewing mDL waiver applications and mDL waiver renewals, purchasing access to industry standards, procuring mDL readers, and mDL training. As displayed in Table 3, the 10-year cost to TSA is $9.84 million undiscounted, $8.62 million discounted at 3 percent, and $7.35 million discounted at 7 percent.

Table 3: Total Cost of the Proposed Rule to DHS ($ Thousands)

Year	Standards Cost	Applicatio n Review Cost	Reappli cation Review Cost	mDL Reader Cost	mDL Training Cost	Total Cost to DHS		
						f = a + b + c + d + e		
	a	b	c	d	e	Undis-counted	Discounted at 3%	Discounted at 7%
1	$0.4	$74.3	$0	$1,418.8	$96.0	$1,589.4	$1,543.1	$1,485.5
2	$0	$49.5	$0	$699.8	$912.9	$1,662.3	$1,566.8	$1,451.9
3	$0	$24.8	$0	$547.9	$601.7	$1,174.4	$1,074.7	$958.6
4	$0	$24.8	$39.9	$440.6	$564.0	$1,069.3	$950.1	$815.8
5	$0	$24.8	$26.6	$240.6	$540.6	$832.6	$718.2	$593.7
6	$0	$0.0	$13.3	$199.4	$455.8	$668.5	$559.9	$445.5

7	$0	$0.0	$53.2	$200.9	$447.6	$701.7	$570.6	$437.0
8	$0	$0.0	$39.9	$202.3	$460.9	$703.2	$555.1	$409.3
9	$0	$0.0	$13.3	$203.8	$474.2	$691.3	$529.8	$376.0
10	$0	$0.0	$53.2	$205.2	$487.5	$745.9	$555.0	$379.2
Total	**$0.4**	**$198.2**	**$239.6**	**$4,359.4**	**$5,041.2**	**$9,838.7**	**$8,623.4**	**$7,352.4**
Annualized							**$1,010.9**	**$1,046.8**

Note: Totals may not add due to rounding.

Relying parties represent Federal agencies that elect to accept a mDLs for official purposes. Per the proposed rule, relying parties would be required to use a mDL reader to retrieve and validate mDL data. As a result, relying parties would incur costs to procure mDL readers should they voluntarily choose to accept mDLs for official purposes. TSA is also considered a relying party, but due to the particular impact to TSA related to the requirement for REAL ID related to boarding federally regulated commercial aircraft, those impacts are discussed separately. As displayed in Table 4, the 10-year cost to relying parties is $3.29 million undiscounted, $2.74 million discounted at 3 percent, and $2.19 million discounted at 7 percent.

Table 4: Total Cost of the Proposed Rule to Relying Parties ($ Thousands)

Year	mDL Reader Cost	Total Cost to Relying Parties		
		b = a		
	a	Undiscounted	Discounted at 3%	Discounted at 7%
1	$39.6	$39.6	$38.5	$37.0
2	$459.4	$459.4	$433.0	$401.2
3	$268.7	$268.7	$245.9	$219.4
4	$190.7	$190.7	$169.4	$145.5
5	$187.5	$187.5	$161.8	$133.7
6	$580.2	$580.2	$485.9	$386.6
7	$370.9	$370.9	$301.6	$231.0
8	$279.2	$279.2	$220.4	$162.5
9	$265.6	$265.6	$203.5	$144.5
10	$644.5	$644.5	$479.6	$327.6
Total	**$3,286.3**	**$3,286.3**	**$2,739.6**	**$2,189.0**
Annualized			**$321.2**	**$311.7**

Note: Totals may not add due to rounding.

TSA has also identified other non-quantified impacts to the affected entities. States may incur costs to: monitor and study mDL technology as it evolves; resolve the underlying issues that could lead to a suspension or termination of a mDL waiver; report serious threats to security, privacy, or data integrity; report material changes to mDL issuance processes; remove conflicts of interest with a third-party auditor; and request reconsideration of a denied mDL waiver application. TSA may incur costs to: investigate circumstances that could lead to suspension or termination of a State's mDL waiver; provide notice to States, relying parties, and the public related to mDL waiver suspensions or terminations; develop an IT solution that maintains an up-to-date list of States with valid mDL waivers; and resolve a request for reconsideration of a denied mDL waiver application. mDL users may incur costs with additional application requirements to obtain a mDL. Relying parties may incur costs to resolve any security or privacy issue with the mDL reader; report serious threats to security, privacy, or data integrity; verifying the list of States with valid mDL waivers; train personnel to verify mDLs; and update the public on identification policies.

TSA believes that States implementing a mDL, absent the rulemaking, would still comply with the AAMVA mDL Implementation Guidelines (hereafter referred to as the "AAMVA Guidelines"). Many of the requirements of the mDL application criteria are already contained within the AAMVA Guidelines. This includes mDL application criteria concerning: data encryption; authentication; device identification keys; user identity verification; applicant presentation; REAL ID compliant physical card; data record; records retention; privacy; and interoperability. Only the mDL application criteria related to escalated review and infrastructure security/issuance are not contained with the AAMVA Guidelines. Operating under the assumption that States interested in mDLs would comply with the AAMVA Guidelines, TSA assumes the application criteria that overlap with the AAMVA Guidelines would otherwise be incurred and thus not

included as a cost of the proposed rule. However, TSA requests comment on this assumption and any cost information associated with the mDL application criteria.

This proposed rule would establish mDL application criteria that would serve as an interim mDL standard for those States choosing to issue mDLs that can be accepted for official purposes. TSA's application criteria may help guide States in their development of mDL technologies which would provide a shared standard that could potentially improve efficiency while also promoting higher security, privacy, and interoperability safeguards.

The application criteria set requirements establishing security and privacy protections to safeguard an mDL holder's identity data. They also set interoperability requirements to ensure secure transactions with Federal agencies. States, via their mDL waiver application, must establish that their mDLs meet the application criteria thus helping to ensure adequate security and privacy protections are in place. Absent the proposed rule, individual States may choose insufficient security and privacy safeguards for mDL technologies that fail to meet the intended security purposes of REAL ID and the privacy needs of users.

mDLs themselves may provide additional security benefits by offering a more secure verification of an individual's identity and authentication of an individual's credential compared to physical cards. In general, mDLs use a cryptographic protocol that ensures the mDL was obtained through a trusted authority, such as a State's Department of Motor Vehicles.[76] This same protocol may prevent the alteration of mDLs and reduce the threat of counterfeit credentials.[77] mDLs also offer increased protection of personal identifiers by preventing over-collection of information. mDLs may possess the

[76] Secure Technology Alliance's Mobile Driver's License Workshop Showcases mDLs Role in the Future of Identification. December 14, 2021. https://www.securetechalliance.org/secure-technology-alliances-mobile-drivers-license-workshop-showcases-mdls-role-in-the-future-of-identification/.
[77] Ibid.

ability to share only those attributes necessary to validate the user identity with the relying party.[78] When using a physical card, the user has no ability to limit the information that is shared, regardless of the amount of information required for verification.

TSA's mDL application criteria can help guide State development and investment in mDLs. The mDL application criteria would foster a level of standardization that would potentially reduce complexity by limiting individual State nuances while also ensuring interoperability across States and with the Federal Government. This increased interoperability reduces implementation costs by limiting the need for different protocols or mechanisms to accept mDLs from individual States.

Identification of mDL application criteria that can be used across States would result in efficiency gains through multiple States pursuing similar objectives, goals, and solutions. Establishing application criteria early in the technology development process has the potential to align development activities across disparate efforts. Early guidance might also reduce re-work or modifications required in future regulations thus saving time and resources redesigning systems and functionality to adhere to subsequent Federal guidelines.

Furthermore, the mDL application criteria may potentially encourage investment in mDLs and the pooling of resources to develop mDL technology capabilities across States and address common concerns or issues. Such collaboration, or unity of effort, can help spread research and development risk and reduce inefficiencies that may arise from States working independently. Greater clarity over mDL regulations, with the proposed rule part of an incremental, multi-phased rulemaking approach, may spur new entrants (States and technology companies) into the mDL ecosystem.

---

[78] Mobile ID can bring both convenience and citizen privacy. July 15, 2021. https://www.biometricupdate.com/202107/mobile-id-can-bring-both-convenience-and-citizen-privacy.

The proposed rule, would allow Federal agencies to continue to accept mDLs for official purposes when REAL ID enforcement begins. This would avoid the sudden halting of mDL acceptance when REAL ID enforcement begins which would reverse trends in providing for a more customer-friendly screening experience. The experience and insight learned through the mDL waiver process could also be used to inform future standards and rulemaking.

3. OMB A-4 Statement

The OMB A-4 Accounting Statement presents annualized costs and qualitative benefits of the proposed rule.

Table 5: **OMB A-4 Accounting Statement ($ Millions, 2022 Dollars)**

Category	Estimates			Units			Notes
	Primary Estimate	Low Estimate	High Estimate	Year Dollar	Discount Rate	Period Covered	
Benefits							
Annualized Monetized ($ millions/year)	N/A	N/A	N/A	N/A	7%	N/A	Not quantified
	N/A	N/A	N/A	N/A	3%	N/A	
Annualized Quantified	N/A	N/A	N/A	N/A	7%	N/A	Not quantified
	N/A	N/A	N/A	N/A	3%	N/A	
Qualitative	The proposed rule, if finalized, would produce benefits by reducing uncertainty in the mDL technology environment by helping to foster a minimum level of security, privacy and interoperability, and reduce potential costs through the alignment of development activities across disparate efforts.						
Costs							
Annualized Monetized ($ millions/year)	$80.01	N/A	N/A	2022	7%	10 years	NPRM Regulatory Impact Analysis (RIA)
	$81.54	N/A	N/A	2022	3%	10 years	
Annualized Quantified	N/A	N/A	N/A	N/A	7%	N/A	Not quantified
	N/A	N/A	N/A	N/A	3%	N/A	
Qualitative	States may incur incremental costs to: monitor and study mDL technology as it evolves; resolve the underlying issues that could lead to a suspension or termination of a mDL waiver; report serious threats to security, privacy, or data integrity; report material changes to mDL issuance processes; remove conflicts of interest with a third-party auditor; and request reconsideration of a denied mDL waiver application. TSA may incur costs to: investigate circumstances that could lead to suspension or termination of a State's mDL waiver; provide notice to States, relying parties, and the public related to mDL waiver suspensions or terminations; develop an IT solution that maintains an up-to-date list of States with valid mDL waivers; and resolve a request for reconsideration of a denied mDL waiver application. mDL users may incur costs with additional application requirements to obtain a mDL. Relying parties may incur costs to resolve any security or privacy issue with the mDL reader; report serious threats to security, privacy, or data integrity; verifying the list of States with valid mDL waivers; train personnel to verify mDLs; and update the public on identification policies.						
Transfers							

From/To	From:	N/A	To:	N/A	
Effects On					
State, Local, and/or Tribal Government	The proposed rule would result in States incurring $813.7 million undiscounted and $552.4 million discounted at 7 percent, in costs over 10 years. The rule would not result in the expenditure by State governments, in the aggregate, of $100 million or more in any one year, as such costs range from $43.0 million to $92.0 million across all States in any given year.				
Small Business	None				NPRM Regulatory Flexibility Analysis (RFA)
Wages	None				
Growth	Not measured				

4. Alternatives Considered

In addition to the proposed rule, or the "preferred alternative", TSA also considered four alternative regulatory options.

The first alternative (Alternative 1) represents the status quo, or no change relative to the proposed creation of a mDL waiver. This represents a scenario without a rulemaking or a waiver process to enable mDL acceptance for official Federal purposes. Under this alternative, States would continue to develop mDLs in a less structured manner while waiting for relevant guiding standards to be published which would likely result in dissimilar mDL implementation and technology characteristics. This alternative was not selected because it does not address the market failures associated with a lack of common standards, such as increased complexity of mDL use across States, and may result in larger costs in the long run when formal mDL standards are finalized.

The second alternative (Alternative 2) features the same requirements of the proposed rule, including an mDL waiver process, but allows for an auto acceptance of certain State waivers that are "low-risk." TSA would identify mDLs from States who have fulfilled the proposed rule's minimum requirements prior to applying for the waiver and have sufficiently demonstrated (*e.g.*, via TSA initiative or recent evaluation by a trusted party) to TSA that their mDL systems present adequate interoperability and low security and privacy risk. The auto acceptance provision would allow Federal agencies to immediately (or conditionally) accept those "low-risk" mDLs for official purposes

pending final approval of the respective State mDL waiver applications. However, TSA rejects this alternative because TSA believes the emerging technology underlying mDLs is insufficiently established to accept the security, privacy, and interoperability of States' mDL systems without an evaluation by TSA or another trusted party. In addition, a similar presumptive eligibility process is not available for other aspects of REAL ID and such an action would not reduce the burden on States or TSA to comply with any framework DHS develops.

Under the third alternative (Alternative 3), TSA would establish more comprehensive requirements than those in the proposed rule to ensure mDLs comply with the REAL ID Act. States would be required to adopt the more comprehensive requirement to issue valid mDLs that can be accepted for official purposes. These technical requirements could include specific standards related to mDL issuance, provisioning, verification, readers, privacy, and other security measures. TSA rejects this alternative because promulgating more comprehensive requirements for mDLs is premature, as both industry standards and technology used by States are still evolving. Restrictive requirements could stifle innovation by forcing all stakeholders to pivot toward compliance. This could impede TSA from identifying and implementing a more efficient regulatory approach in the future.

Finally, under the fourth alternative (Alternative 4), instead of a waiver process, TSA would first establish minimum requirements for issuing REAL ID compliant mDLs before TSA later sets more comprehensive requirements as additional guidance and standards become available in the mid- and long-term. The interim minimum requirements would consist of the same requirements for security, privacy, and interoperability, based on nineteen industry and government standards and guidelines, described in the proposed rule to guide waiver applications. Alternative 4 effectively would codify standards that may become obsolete in the near future, as existing standards

are revised, emerging standards publish, and new cyber threats proliferate. TSA rejects this alternative because establishing minimum requirements that may become obsolete in the near future may limit the ability for TSA to revise standards quickly and would increase the security and privacy risks of accepting mDLs. In addition, costs under Alternative 4 would roughly be similar to costs under the proposed rule, as both options would require audits and other compliance costs. TSA requests comments as to whether finalizing these minimum requirements for REAL ID compliance would be preferable to the temporary waiver process described in this proposal. Specifically, TSA seeks comment on whether Alternative 4 would realize higher benefits, either quantitative or qualitative, for States and the public, than the waiver process described in this proposal. TSA also seeks comment on costs to the affected entities to comply with the minimum requirements.

5. Regulatory Flexibility Act Assessment

The Regulatory Flexibility Act (RFA) of 1980, as amended,[79] was enacted by Congress to ensure that small entities (small businesses, small not-for-profit organizations, and small governmental jurisdictions) would not be unnecessarily or disproportionately burdened by Federal regulations. Section 605 of the RFA allows an agency to certify a rule in lieu of preparing an analysis if the regulations are not expected to have a significant economic impact on a substantial number of small entities.

In accordance with the RFA, TSA has not prepared a Regulatory Flexibility Analysis and pursuant to 5 U.S.C. 605(b), the Secretary certifies that the proposed rule would not have a significant economic impact on a substantial number of small entities. The proposed rule would directly impact States that voluntarily choose to apply for a

[79] Public Law 96-354, 94 Stat. 1164 (Sept. 19, 1980) (codified at 5 U.S.C. 601 *et seq*., as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA)).

waiver that would permit mDLs issued by those States to be accepted for official Federal purposes.

6. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. The Trade Agreement Act does not consider legitimate domestic objectives, such as essential security, as unnecessary obstacles. The statute also requires that international standards be considered and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this proposed rule and has determined this rule would not have an adverse impact on international trade.

7. Unfunded Mandates Reform Act Assessment

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), Public Law 104–4, establishes requirements for Federal agencies to assess the effects of their regulatory actions on State, local, and tribal governments and the private sector. Under sec. 202 of the UMRA, TSA generally must prepare a written Statement, including a cost-benefit analysis, for proposed and final rules with "Federal mandates" that may result in expenditures by State, local, and tribal governments in the aggregate or by the private sector of $100 million or more (adjusted for inflation) in any one year.

Before TSA promulgates a rule for which a written statement is required, sec. 205 of the UMRA generally requires TSA to identify and consider a reasonable number of regulatory alternatives and adopt the least costly, most cost-effective, or least burdensome alternative that achieves the objectives of the rulemaking. The provisions of sec. 205 do not apply when they are inconsistent with applicable law. Moreover, sec. 205 allows TSA to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the final rule provides an explanation why that alternative was

not adopted. Before TSA establishes any regulatory requirements that may significantly or uniquely affect small governments, including tribal governments, it must develop under sec. 203 of the UMRA a small government agency plan. The plan must provide for notifying potentially affected small governments, enabling officials of affected small governments to have meaningful and timely input in the development of TSA regulatory proposals with significant Federal intergovernmental mandates, and informing, educating, and advising small governments on compliance with the regulatory requirements.

When adjusted for inflation, the threshold for expenditures becomes $177.1 million in 2022 dollars. TSA has determined that this proposed rule does not contain a Federal mandate that may result in expenditures that exceed that amount either for State, local, and tribal governments in the aggregate in any one year. TSA will publish a final analysis, including its response to public comments, when it publishes a final rule.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq*.) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public. Under the provisions of PRA section 3507(d), DHS must obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. This proposed rule would call for a collection of information under the PRA. Accordingly, TSA has submitted to OMB the proposed rule and this analysis, including the sections relating to collections of information. *See* 5 CFR 1320.11(a). As defined in 5 CFR 1320.3(c), "collection of information" includes reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. This section provides the description of the information collection and of those who must collect the information as well as an estimate of the total annual time burden.

The proposed rule establishes a process for States to apply to TSA for a temporary waiver. Such a request is voluntary but would require the submission of an mDL waiver application, resubmission of an mDL waiver application deemed insufficient or denied, and reapplication for a mDL waiver when the term of the mDL waiver expires. All of these items would be considered new information collections.

TSA uses the current State of mDL implementation to inform its estimate on how many State entities would request a mDL waiver during the period of analysis.[80] All 50 States, the District of Columbia, and five territories (collectively referred to as States hereafter) are eligible to apply for a mDL waiver as discussed in the proposed rule. However, DHS assumes that not all States would apply for the mDL waiver. TSA assumes 15 States would apply for a mDL waiver in Year 1 of the analysis, 10 States in Year 2, and five States in Year 3.[81]

Following the State submission of its mDL waiver application, TSA determines if the application is approved, insufficient, or denied. States are allowed to amend an insufficient or denied mDL waiver application and resubmit to TSA review.

TSA assumes that all submissions would initially be deemed insufficient due to the mDL waiver criteria being new and with mDLs an emerging technology. Nonetheless, TSA intends to work individually with interested States to meet the mDL criteria to maximize the likelihood of receiving a waiver. Based on these assumptions, TSA estimates all initial mDL waiver applications would be deemed insufficient and that 90 percent of States would resubmit their mDL waiver applications.[82]

---

[80] Eight States currently provide mDLs. Roughly 20 States have taken steps towards mDL implementation, including seven States participating in the TSA mobile ID evaluation program without a current mDL solution.

[81] Each State would submit one mDL waiver application.

[82] DHS assumes that 10 percent of applications deemed insufficient would no longer pursue a mDL waiver due to the level of effort involved to become sufficient and wait until the mDL environment is more fully developed.

A State's mDL waivers would be valid for three years. Therefore, States granted a mDL waiver in Year 1 would need to reapply in Year 4 which is beyond the scope of this particular information collection.

TSA technology subject matter experts estimate that the mDL waiver application would take, on average, 20 hours to complete. TSA also estimates that mDL waiver resubmissions would take 25 percent of the initial mDL waiver application time which equates to 5 hours.[83] Finally, TSA estimates that mDL waiver reapplications would take 75 percent of the initial mDL waiver application time which equates to 15 hours.[84]

These hour burden estimates are combined with the number of collection activities to calculate the total and average time burden associated with the proposed rule. TSA estimates the proposed rule's total three-year burden for mDL waiver applications, mDL waiver resubmissions, and mDL waiver reapplications is 57 responses and 735 hours. TSA estimates an average yearly burden of 19 responses and 245 hours. Details of the calculation can be found in Table 6.

Table 6: PRA Information Collection Responses and Burden Hours

Collection Activity	Number of Responses						Total Hours	Average Annual Hours
	Year1	Year 2	Year 3	Total Responses	Average Annual Responses	Time Per Response (hours)		
	a	b	c	d = a + b + c	e = d / 3	f	g = d * f	h = g / 3
mDL Waiver Application	15.0	10.0	5.0	30.0	10.0	20	600	200
mDL Waiver Resubmission	13.5	9.0	4.5	27.0	9.0	5	135	45
mDL Waiver Reapplication	0	0	0	0	0	15	0	0
Total	**28.5**	**19.0**	**9.5**	**57.0**	**19.0**		**735**	**245**

In addition, States TSA incur costs associated with independent entity audits of their mDL infrastructure. DHS estimates this cost at $32,500 per submission.[85] States

[83] mDL Waiver Resubmission burden = 20 hours [initial mDL waiver application burden] x 0.25 = 5 hours.
[84] mDL Waiver Renewal burden = 20 hours [initial mDL waiver application burden] x (1 - 0.25) = 15 hours.
[85] TSA technology subject matter experts assume estimate a range of audit costs between $5,000 and $60,000. DHS uses the midpoint of this range as the point estimate.

would incur this cost for the initial mDL waiver application and mDL waiver reapplication. As there are no reapplications anticipated for this information collection request, TSA multiplies the annual average number of mDL waiver applications from Table 6 above (10) and the independent entity audit cost of $32,500 for a total mDL waiver application cost of $325,000.

C. Federalism (E.O. 13132)

A rule has implications for federalism under E.O. 13132 of August 6, 1999 (Federalism) if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. TSA analyzed this proposed rule under this order and determined it does not have these implications for federalism.

D. Customer Service (E.O. 14058)

E.O. 14058 of December 13, 2021 (Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government), is focused on enhancing the of technology "to modernize Government and implement services that are simple to use, accessible, equitable, protective, transparent, and responsive for all people of the United States." The Secretary of Homeland Security has specifically committed to testing the use of innovative technologies at airport security checkpoints to reduce passenger wait times. This proposed rule supports this commitment. Using mDLs to establish identity at airport security checkpoints is intended to provide the public with increased convenience, security, privacy, and health benefits from "contact-free" identity verification. In 2022, DHS began a limited initiative to evaluate some mDLs to determine the viability of using an mDLs as a form of identification at an airport security checkpoint.

E. Energy Impact Analysis (E.O. 13211)

TSA analyzed this proposed rule under E.O. 13211 of May 18, 2001 (Actions Concerning Regulations That Significantly Affected Energy Supply, Distribution or Use),

and determined that it is not a "significant energy action" under that E.O. and is not likely to have a significant adverse effect on the supply, distribution, or use of energy. Therefore, this rulemaking does not require a Statement of Energy Effects.

F. Environmental Analysis

TSA reviews proposed actions to determine whether the National Environmental Policy Act (NEPA) applies to them and, if so, what degree of analysis is required. DHS Directive 023–01 Rev. 01 (Directive) and Instruction Manual 023–01–001–01 Rev. 01 (Instruction Manual) establish the procedures that DHS and its components use to comply with NEPA and the Council on Environmental Quality (CEQ) regulations for implementing NEPA, 40 CFR parts 1500 through 1508. The CEQ regulations allow Federal agencies to establish, with CEQ review and concurrence, categories of actions (''categorical exclusions'') which experience has shown do not individually or cumulatively have a significant effect on the human environment and, therefore, do not require an Environmental Assessment (EA) or Environmental Impact Statement (EIS). *See* 40 CFR 1507.3(b)(2)(ii), 1508.4. DHS has determined that this action will not have a significant effect on the human environment. This action is covered by categorical exclusion number A3(d) in DHS Management Directive 023-01 Rev. 01.

VII. Specific Questions

While commenters are asked to comment on this proposal in its entirety, TSA specifically requests comments in response to the following questions. Commenters are encouraged to address issues that may not be discussed below based upon their knowledge of the issues and implications. In providing your comments, please follow the instructions in the Commenter Instructions section above.

1. Applications for waivers. Provide comments on:

a. The estimated cost and time required for States to complete and submit applications for waivers, including the initial mDL waiver application, resubmission, and reapplication;

b. The estimated number of States and territories that would submit a waiver application, and when those States and territories would submit a waiver application;

c. The percentage of States that would receive a decision of approved, insufficient, or denied;

d. The percentage of States receiving a decision of insufficient that would resubmit an amended application; and

e. The assumption that TSA would approve all resubmitted applications.

2. Application Criteria. Provide comments on:

a. The costs States may incur to demonstrate compliance with the criteria to apply for a waiver as required by proposed § 37.10(a) and appendix A to subpart A of the part, including the costs and availability of any professional services required;

b. The appropriateness of the application requirements set forth in proposed § 37.10(a) and appendix A to subpart A of the part;

c. The impact that the Initial Public Versions of Revision 4 of NIST SP 800-63, NIST SP 800-63A, NIST SP 800-63B, and NIST SP 800-63C may have on the requirements set forth in proposed § 37.10(a) and appendix A to subpart A of the part, including States' ability to demonstrate compliance with the criteria to apply for a waiver as required by proposed § 37.10(a) and appendix A to subpart A of the part.

3. Audit report. Provide comments on requiring States to submit a report of an audit as required in proposed § 37.10(b), which report would require verifying the materials that a State would provide in its application for a waiver as required by proposed § 37.10(a), including:

a. The appropriateness of requiring an audit to be conducted by a recognized independent entity;

b. The appropriateness of requiring an auditor to hold an active Certified Public Accountant license in the State that is seeking a waiver;

c. The appropriateness of requiring an auditor to be experienced with information systems security audits, including whether such auditors should have different or additional experience;

d. The appropriateness of requiring the auditor to be accredited by the State seeking a waiver;

e. The appropriateness of requiring an auditor to hold a current and active American Institute of Certified Public Accountants (AICPA) Certified Information Technology Professional (CITP) credential or ISACA (F/K/A Information Systems Audit and Control Association) Certified Information System Auditor certification;

f. The availability of auditors who meet the criteria specified in proposed § 37.10(b)(1);

g. The estimated cost and time incurred by States to obtain a report by the auditor; and

h. Any other considerations relating to auditing.

4. DHS Mobile Driver's License Waiver Application Guidance. Provide comments on the "Mobile Driver's License Waiver Application Guidance," available at www.dhs.gov/real-id/mDL.

5. Waiver validity period. DHS is considering a three-year validity period for waivers. Provide comments on the appropriateness of a three-year validity period for waivers and on alternate validity periods.

6. Mobile driver's license readers. Provide comment on the costs to procure mDL reader equipment, estimated reader usage by Federal agencies, States, and businesses, and the functional form of such reader equipment.

7. mDL acceptance. Provide comment on the number of Federal agencies other than TSA DHS and DHS component agencies that voluntarily choose to accept mDLs for official purposes for identity verification, including:

a. The number and types of locations where mDLs will be accepted; and

b. The number of individuals that are expected to obtain mDLs.

8. Costs to individuals. Provide comment on costs incurred by mDL users, including costs associated with obtaining an mDL.

9. TSA invites public comments on Alternative 4, including, but not limited to, costs to the affected entities to comply with the minimum standards, benefits of the alternative compared to the preferred alternative, and risks to security and privacy of accepting mDLs based on the minimum requirements.

List of Subjects in 6 CFR Part 37

Document security, Driver's licenses, Identification cards, Incorporation by reference, Licensing and registration, Motor vehicle administrations, Motor vehicle safety, Motor vehicles, Personally identifiable information, Physical security, Privacy, Reporting and recordkeeping requirements, Security measures.

The Proposed Amendments

For the reasons set forth in the preamble, the Transportation Security Administration is proposing to amend part 37 of title 6, Code of Federal Regulations, to read as follows:

PART 37—REAL ID DRIVER'S LICENSES AND IDENTIFICATION CARDS

1. The authority citation for part 37 continues to read as follows:

Authority: 49 U.S.C. 30301 note; 6 U.S.C. 111, 112.

Subpart A—General

2. Amend § 37.3 by adding the definitions for "A Root Certificate Authority," "Administration," "Certificate Authority," "Certificate Management System," "Certificate Policy," "Certificate System," "Critical Security Event," "Delegated Third Party," "Delegated Third Party System," "Denial of Service," "Digital Certificates," "Digital Signatures," "Distributed Denial of Service," "Execution Environment," "Front End System," "Hardware security module," "High Security Zone," "Identity Proofing," "Identity verification," "Internal Support System," "Issuing Authority," "Issuing Authority Certificate Authority," "Issuing System," "mDL," "Mobile driver's license," "Mobile identification card," "Multi-Factor Authentication," "Online Certificate Status Protocol," "Penetration Test," "Public Key Infrastructure," "Rich Execution Environment," "Root Certificate Authority System," "Secure Element," "Secure hardware," "Secure Key Storage Device," "Secure Zone," "Security Support System," "Sole Control," "State Root Certificate," "System," "Trusted Execution Environment," "Trusted Role," "Virtual Local Area Network," "Vulnerability," "Vulnerability scanning," and "Zone" in alphabetical order to read as follows:

§ 37.3 Definitions.

* * * * *

A Root Certificate Authority is the State *Certificate Authority* whose public encryption key establishes the basis of trust for all other *Digital Certificates* issued by a State.

Administration means management actions performed on *Certificate Systems* by a person in a *Trusted Role*.

* * * * *

Certificate Authority means an issuer of *Digital Certificates* that are used to certify the identity of parties in a digital transaction.

Certificate Management System means a system used by a State or *Delegated Third Party* to process, approve issuance of, or store *Digital Certificates* or Digital Certificate status information, including the database, database server, and storage.

Certificate Policy means the set of rules and documents that forms a State's governance framework in which *Digital Certificates*, *Certificate Systems*, and cryptographic keys are created, issued, managed, and used.

Certificate System means the system used by a State or *Delegated Third Party* to provide services related to *Public Key Infrastructure* for digital identities.

* * * * *

Critical Security Event means detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a *Zone's* security controls or a compromise of a *Certificate System's* integrity, including excessive login attempts, attempts to access prohibited resources, *Denial of Service* or *Distributed Denial of Service* attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or an actual compromise of component integrity.

* * * * *

Delegated Third Party means a natural person or legal entity that is not the State and that operates any part of a *Certificate System* under the State's legal authority.

Delegated Third Party System means any part of a *Certificate System* used by a *Delegated Third Party* while performing the functions delegated to it by the State.

Denial of Service means the prevention of authorized access to resources or the delaying of time-critical operations.

* * * * *

Digital Certificates identify the parties involved in an electronic transaction, and contain information necessary to validate *Digital Signatures*.

Digital Signatures are mathematical algorithms used to validate the authenticity and integrity of a message.

Distributed Denial of Service means a *Denial of Service* attack where numerous hosts perform the attack.

* * * * *

Execution Environment means a place within a device processer where active application's code is processed.

* * * * *

Front End System means a system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.

* * * * *

Hardware security module means a physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing.

High Security Zone means a physical location where a State's or *Delegated Third Party's* private key or cryptographic hardware is located.

* * * * *

Identity Proofing refers to a series of steps that the State executes to prove the identity of a person.

Identity verification is the confirmation that identity data belongs to its purported holder.

* * * * *

Internal Support System means a system which operates on a State's internal network and communicates with the *Certificate System* to provide business services related to mDL management.

Issuing Authority means the State that issues a *mobile driver's license* or *mobile identification card*.

Issuing Authority Certificate Authority means a *Certificate Authority* operated by or on behalf of an *Issuing Authority* or a State's *Root Certificate Authority*.

Issuing System means a system used to sign mDLs, digital certificates, mobile security objects, or validity status information.

* * * * *

mDL means *mobile driver's licenses* and *mobile identification cards*, collectively.

Mobile driver's license means a *driver's license* that is stored on a mobile electronic device and read electronically.

Mobile identification card means an *identification card*, issued by a State, that is stored on a mobile electronic device and read electronically.

Multi-Factor Authentication means an authentication mechanism consisting of two or more of the following independent categories of credentials (i.e., factors) to verify the user's identity for a login or other transaction means something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor).

* * * * *

Online Certificate Status Protocol means an online protocol used to determine the status of a *Digital Certificate*.

* * * * *

Penetration Test means a process that identifies and attempts to exploit vulnerabilities in systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

* * * * *

Public Key Infrastructure means a structure where a *Certificate Authority* uses *Digital Certificates* for issuing, renewing, and revoking digital credentials.

* * * * *

Rich Execution Environment, also known as a "normal execution environment," means the area inside a device processor that runs an operating system.

Root Certificate Authority System means a system used to create a State's *Root Certificate* or to generate, store, or sign with the private key associated with a *State Root Certificate.*

* * * * *

Secure Element means a tamper-resistant secure hardware component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models.

Secure hardware means hardware provided on a mobile device for key management and trusted computation such as a *Secure Element* (SE) or *Trusted Execution Environment*.

Secure Key Storage Device means a device certified as meeting the specified FIPS 140-3 Level 2 overall, Level 3 physical, or Common Criteria (EAL 4+).

Secure Zone means an area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of *Certificate Systems.*

Security Support System means a system used to provide security support functions, which may include authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (host-based intrusion detection, network-based intrusion detection).

* * * * *

Sole Control means a condition in which logical and physical controls are in place to ensure the *Administration* of a *Certificate System* can only be performed by a State or *Delegated Third Party.*

* * * * *

State Root Certificate means a public *Digital Certificate* of a *Root Certificate Authority* operated by or on behalf of a State.

System means one or more pieces of equipment or software that stores, transforms, or communicates data.

* * * * *

Trusted Execution Environment means an *Execution Environment* that runs alongside but isolated from a *Rich Execution Environment* and has the security capabilities necessary to protect designated applications.

Trusted Role means an employee or contractor of a State or *Delegated Third Party* who has authorized access to or control over a *Secure Zone* or *High Security Zone.*

* * * * *

Virtual Local Area Network means a broadcast domain that is partitioned and isolated within a network.

Vulnerability means a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability scanning means a technique used to identify host attributes and associated *Vulnerabilities*.

Zone means a subset of *Certificate Systems* created by the logical or physical partitioning of systems from other *Certificate Systems.*

3. Amend § 37.4 by adding paragraphs (a)(2), (b)(2), and (d) through (f) to read as follows:

§ 37.4 Incorporation by reference.

*****

(a)***

(2) ISO/IEC 18013-5:2021, Personal identification — ISO-compliant driving license — Part 5: Mobile driving license (mDL) application, Edition 1 (September 2021); IBR approved for §§ 37.8; 37.10(a); appendix A to this subpart.

(b) ***

(2) Mobile Driver's License (mDL) Implementation Guidelines, Version 1.2 (January 2023); IBR approved for § 37.10(a); appendix A to this subpart.

*****

(d) Certification Authority Browser Forum (CA/Browser Forum), 815 Eddy St, San Francisco, CA 94109, (415) 436-9333, questions@cabforum.org, www.cabforum.org.

(1) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 1.8.6 (December 14, 2022), https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.6.pdf; IBR approved for appendix A to this subpart.

(2) Network and Certificate System Security Requirements, Version 1.7 (April 5, 2021), https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf; IBR approved for appendix A to this subpart A.

(e) Cybersecurity and Infrastructure Security Agency, Mail Stop 0380, Department of Homeland Security, 245 Murray Lane, Washington, D.C. 20528-0380, central@cisa.gov, (888) 282-0870, www.cisa.gov.

(1) Cybersecurity Incident & Vulnerability Response Playbooks (November 2021), https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity

_Incident_and_Vulnerability_Response_Playbooks_508C.pdf; IBR approved for appendix A to this subpart.

(2) National Cyber Incident Response Plan (December 2016), Department of Homeland Security, https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf; IBR approved for appendix A to this subpart.

(f) National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, (301) 975-2000, www.nist.gov.

(1) Federal Information Processing Standard (FIPS) Publication (PUB) 140-3, Security Requirements for Cryptographic Modules (March 22, 2019), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf; IBR approved for appendix A to this subpart.

(2) FIPS PUB 180-4, Secure Hash Standard (SHS) (August 2015), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf; IBR approved for § 37.10(a).

(3) FIPS PUB 186-5, Digital Signature Standard (DSS) (Feb. 2023), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf; IBR approved for § 37.10(a).

(4) FIPS PUB 197, Advanced Encryption Standard (AES) (Nov. 26, 2001), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf; IBR approved for § 37.10(a).

(5) FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC) (July 2008), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf; IBR approved for § 37.10(a).

(6) FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (August 2015), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf; IBR approved for § 37.10(a).

(7) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, Rev. 5 (September 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53 Rev. 5.pdf; IBR approved for appendix A to this subpart.

(8) SP 800-57 Part 1, Recommendation for Key Management: Part 1 – General, Rev. 5, Elaine Barker (May 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf; IBR approved for appendix A to this subpart.

(9) SP 800-57 Part 2, Recommendation for Key Management: Part 2 – Best Practices for Key Management Organization, Rev. 1, Elaine and William C. Barker (May 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf; IBR approved for appendix A to this subpart A.

(10) SP 800-57 Part 3, Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance, Rev. 1, Elaine Barker and Quynh Dang (January 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf; IBR approved for appendix A to this subpart.

(11) SP 800-63-3, Digital Identity Guidelines, Paul A. Grassi et al. (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf; IBR approved for appendix A to this subpart.

(12) SP 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management, Paul A. Grassi et al. (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf; IBR approved for appendix A to this subpart.

(13) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (April 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; IBR approved for appendix A to this subpart.

3. Add § 37.7 to read as follows:

§ 37.7 Temporary waiver for mDLs; State eligibility.

(a) *Generally.* TSA may issue a temporary certificate of waiver that exempts mDLs issued by a State from meeting the requirements in § 37.5(b), when the State meets the requirements of § 37.10(a) and (b).

(b) *State eligibility*. A State may be eligible for a waiver only if, after considering all information provided by a State under § 37.10(a) and (b), TSA determines that—

(1) The State is in full compliance with all applicable REAL ID requirements as defined in subpart E of this part;

(2) Information provided by the State under § 37.10(a) and (b) sufficiently demonstrates that the State's mDL provides the security, privacy, and interoperability necessary for acceptance by Federal agencies; and

(3) The State issues mDLs only to individuals who have been issued a valid and unexpired REAL ID-compliant physical driver's license or identification card issued by that State.

4. Add § 37.8 to read as follows:

§ 37.8 Requirements for Federal agencies accepting mDLs issued by States with temporary waiver.

Notwithstanding § 37.5(b), Federal agencies may accept an mDL for REAL ID official purposes issued by a State that has a valid certificate of waiver issued by TSA under § 37.7(a). A Federal agency that elects to accept mDLs under this section must—

(a) Confirm the State holds a valid certificate of waiver consistent with § 37.7(a) by verifying that the State appears in a list of mDLs approved for Federal use, available as provided in § 37.9(b)(1);

(b) Use an mDL reader to retrieve and validate mDL data as required by standard ISO/IEC 18013-5:2021 (incorporated by reference; see § 37.4); and

(c) Upon discovery that acceptance of a State's mDL is likely to cause imminent or serious threats to the security, privacy, or data integrity, the agency's senior official responsible for REAL ID compliance, or equivalent function, must report such discovery to DHS at www.dhs.gov/real-id/mDL within 72 hours of such discovery.

5. Add § 37.9 to read as follows:

§ 37.9 Applications for temporary waiver for mDLs.

(a) *Application process*. Each State requesting a temporary waiver must file with TSA a complete application as set forth in § 37.10(a) and (b). Application filing instructions, may be obtained from DHS at www.dhs.gov/real-id/mDL.

(b) *Decisions*. TSA will provide written notice via email to States within 60 days, to the extent practicable, but in no event longer than 90 days, indicating that TSA has made one of the following decisions:

(1) *Approved*. Upon approval of an application for a temporary waiver, TSA will issue a certificate of waiver to the State, and publish the State's name in a list of mDLs approved for Federal use at www.dhs.gov/real-id/mDL.

(2) *Insufficient*. Upon determination that an application for a temporary waiver is incomplete or otherwise deficient, TSA will provide the State an explanation of deficiencies, and an opportunity to address any deficiencies and submit an amended application. States will have 60 days to respond to the notice, and TSA will respond via email within 30 days.

(3) *Denied*. Upon determination that an application for a waiver fails to meet criteria specified in § 37.10(a) and (b), TSA will provide the State specific grounds on which the denial is based, and provide the State an opportunity to seek reconsideration as provided in paragraph (c) of this section.

(c) *Reconsideration*. (1) States will have 90 days to file a request for reconsideration of a denied application. The State must explain what corrective action it intends to implement to correct any defects cited in the denial or, alternatively, explain why the denial is incorrect. Instructions on how to file a request for reconsideration for denied applications may be obtained from TSA at www.dhs.gov/real-id/mDL. TSA will notify States of its final determination within 60 days of receipt of a State's request for reconsideration.

(2) An adverse decision upon reconsideration is a final agency action. A State whose request for reconsideration has been denied may submit a new application at any time following the process set forth in paragraph (a) of this section.

(d) *Terms and conditions*. A certificate of waiver will specify—

(1) The effective date of the waiver;

(2) The expiration date of the waiver; and

(3) Any additional terms or conditions as necessary.

(e) *Limitations; suspension; termination*--(1) *Validity period*. A certificate of waiver is valid for a period of 3 years from the date of issuance.

(2) *Reporting requirements.* If a State, after it has been granted a certificate of waiver, makes any significant additions, deletions, or modifications to its mDL issuance processes, other than routine systems maintenance and software updates, that differ materially from the information the State provided in response to § 37.10(a) and (b) under which the waiver was granted, the State must provide written notice of such

changes to TSA at www.dhs.gov/real-id/mDL 60 days before implementing such additions, deletions, or modifications.

(3) *Compliance*. A State that is issued a certificate of waiver under this section must comply with all applicable REAL ID requirements in § 37.51(a), and with all terms and conditions specified in paragraph (d)(3) of this section.

(4) *Suspension.* (i) TSA may suspend the validity of a certificate of waiver for any of the following reasons:

(A) *Failure to comply*. TSA determines that a State has failed to comply with paragraph (d)(3) or (e)(2) of this section, or has issued mDLs in a manner not consistent with the information provided under § 37.10(a) or (b); or

(B) *Threats to security, privacy, and data integrity*. TSA reserves the right to suspend a certificate of waiver at any time upon discovery that Federal acceptance of a State's mDL is likely to cause imminent or serious threats to the security, privacy, or data integrity of any Federal agency. In such instances, TSA will provide written notice via email to each affected State as soon as practicable after discovery of the triggering event, including reasons for suspension, an explanation of any corrective actions a State must take to resume validity of its certificate of waiver.

(ii) Before suspending a certificate of waiver under paragraph (e)(4)(i)(A) of this section, TSA will provide to such State written notice via email of intent to suspend, including an explanation of deficiencies and instructions on how the State may cure such deficiencies. States will have 30 days to respond to the notice, and TSA will respond via email within 30 days. TSA's response would include one of the following: withdrawal of the notice, a request for additional information, or a final suspension.

(iii) If TSA issues a final suspension, TSA will temporarily remove the State from the list of mDLs approved for Federal acceptance for official purposes. TSA will continue to work with a State to whom TSA has issued a final suspension to resume

validity of its existing certificate of waiver. A State that has been issued a final suspension may seek a new certificate of waiver by submitting a new application following the process set forth in paragraph (a) of this section.

(5) *Termination*. (i) DHS may terminate a certificate of waiver at an earlier date than specified in paragraph (d)(2) of this section if TSA determines that a State—

(A) Does not comply with applicable REAL ID requirements in § 37.51(a);

(B) Is committing an egregious violation of requirements specified under paragraph (d)(3) or (e)(2) of this section that the State is unwilling to cure; or

(C) Provided false information in support of its waiver application.

(ii) Before terminating a certificate of waiver, TSA will provide the State written notice via email of intent to terminate, including findings on which the intended termination is based, together with a notice of opportunity to present additional information. States must respond to the notice within 7 days, and TSA will reply via email within 30 days. TSA's response would include one of the following: withdrawal of the notice, a request for additional information, or a final termination.

(iii) If TSA issues a final termination, TSA will remove the State from the list of mDLs approved for Federal acceptance for official purposes. A State whose certificate of waiver has been terminated may seek a new waiver by submitting a new application following the process set forth in paragraph (a) of this section.

(6) *Reapplication*. A State seeking extension of a certificate of waiver after expiration of its validity period must file a new application under paragraph (a) of this section.

(f) *Effect of status of certificate of waiver.* (1) Issuance of a certificate of waiver is not a determination of compliance with any other section in this part.

(2) An application for certificate of waiver that TSA has deemed insufficient or denied, or a certificate of waiver that TSA has deemed suspended, terminated, or expired, is not a determination of non-compliance with any other section in this part.

6. Add § 37.10 to read as follows:

§ 37.10 Application criteria for issuance of temporary waiver for mDLs; audit report; waiver application guidance.

(a) *Application criteria*. A State requesting a certificate of waiver must establish in its application that the mDLs for which the State seeks a waiver are issued with controls sufficient to resist compromise and fraud attempts, provide privacy protections sufficient to safeguard an mDL holder's identity data, and provide interoperability for secure acceptance by Federal agencies under the terms of a certificate of waiver. To demonstrate compliance with such requirements, a State must provide information, documents, and/or data sufficient to explain the means, which includes processes, methodologies, or policies, that the State has implemented to comply with requirements in this paragraph (a).

(1) *Provisioning*. For both remote and in-person provisioning, a State must explain the means it uses to address or perform the following—

(i) *Data encryption*. Securely encrypt mDL data and an mDL holder's Personally Identifiable Information when such data is transferred during provisioning, and when stored on the State's system(s) and on mDL holders' mobile devices.

(ii) *Escalated review*. Review repeated failed attempts at provisioning, resolve such failures, and establish criteria to determine when the State will deny provisioning an mDL to a particular mDL applicant.

(iii) *Authentication*. Confirm that an mDL applicant has control over the mobile device to which an mDL is being provisioned at the time of provisioning.

(iv) *Device identification keys.* Confirm that the mDL applicant possesses the mDL device private key bound to the mDL during provisioning.

(v) *User identity verification*. Prevent an individual from falsely matching with the licensing agency's records, including portrait images, of other individuals.

(vi) *Applicant presentation*. Prevent physical and digital presentation attacks by detecting the liveness of an individual and any alterations to the individual's appearance during remote and in-person provisioning.

(vii) *REAL ID compliant physical card*. Issue mDLs only to residents who have been issued by that State a valid and unexpired REAL ID compliant physical driver's license or physical identification card.

(viii) *Data record*. Issue mDLs using data, including portrait image, of an individual that matches corresponding data in the database of the issuing State's driver's licensing agency for that individual.

(ix) *Records retention*. Manage mDL records and related records, consistent with requirements set forth in the American Association of Motor Vehicle Administrator (AAMVA) Mobile Driver's License (mDL) Implementation Guidelines (incorporated by reference; see § 37.4).

(2) *Issuance*. A State must explain the means it uses to manage the creation, issuance, use, revocation, and destruction of the State's certificate systems and keys in full compliance with the requirements set forth in appendix A to this subpart.

(3) *Privacy*. A State must explain the means it uses to protect Personally Identifiable Information during processing, storage, and destruction of mDL records and provisioning records.

(4) *Interoperability*. A State must explain the means it uses to issue mDLs that are interoperable with standard ISO/IEC 18013-5:2021 and the "AAMVA mDL data element set" defined in the American Association of Motor Vehicle Administrator

(AAMVA) Mobile Driver's License (mDL) Implementation Guidelines v. 1.1 (incorporated by reference; see § 37.4) as follows:

(i) A State must issue mDLs using the data model defined in ISO/IEC 18103-5:2021 section 7 (incorporated by reference; see § 37.4), using the document type "org.iso.18013.5.1.mDL," and using the name space "org.iso.18013.5.1". States must include the following mDL data elements defined as mandatory in Table 5: "family_name", "given_name", "birth_date", "issue_date", "expiry_date", "issuing_authority", "document_number", "portrait", and must include the following mDL data elements defined as optional in Table 5: "sex", "resident_address", "portrait_capture_date", "signature_usual_mark".

(ii) States must use the AAMVA mDL data element set defined in American Association of Motor Vehicle Administrator (AAMVA) Mobile Driver's License (mDL) Implementation Guidelines v. 1.2, Section 3.2 (incorporated by reference; see § 37.4), using the namespace "org.iso.18013.5.1.aamva" and must include the following data elements in accordance with the AAMVA mDL Implementation Guidelines v1.2 (incorporated by reference; see § 37.4): "DHS_compliance", and "DHS_temporary_lawful_status".

(iii) States must use only encryption algorithms, secure hashing algorithms, and digital signing algorithms as defined by ISO/IEC 18103-5:2021, Section 9 and Annex B (incorporated by reference; see § 37.4), and which are included in the following NIST Federal Information Processing Standards (FIPS): NIST FIPS PUB 180-4, NIST FIPS PUB 186-5, NIST FIPS PUB 197, NIST FIPS PUB 198-1, and NIST FIPS PUB 202 (incorporated by reference; see § 37.4).

(b) *Audit report.* States must include with their applications a report of an audit that verifies the information provided under paragraph (a) of this section.

(1) The audit must be conducted by a recognized independent entity—

(i) Holding an active Certified Public Accountant license in the issuing State;

(ii) Experienced with information systems security audits;

(iii) Accredited by the issuing State; and

(iv) Holding a current and active American Institute of Certified Public Accountants (AICPA) Certified Information Technology Professional (CITP) credential or ISACA (F/K/A Information Systems Audit and Control Association) Certified Information System Auditor (CISA) certification.

(2) States must include information about the entity conducting the audit that identifies—

(i) Any potential conflicts of interest; and

(ii) Mitigation measures or other divestiture actions taken to avoid conflicts of interest.

(c) *Waiver application guidance*--(1) *Generally*. TSA will publish "Mobile Driver's License Waiver Application Guidance" to facilitate States' understanding of the requirements set forth in paragraph (a) of this section. The non-binding Guidance will include recommendations and examples of possible implementations for illustrative purposes only. TSA will publish the Guidance on the REAL website at www.dhs.gov/real-id/mDL.

(2) *Updates*. TSA may periodically update its Waiver Application Guidance as necessary to provide additional information or recommendations to mitigate evolving threats to security, privacy, or data integrity. TSA will publish updated Guidance in the *Federal Register* and at www.dhs.gov/real-id/mDL, and provide a copy to all States that have applied for or been issued a certificate or waiver.

7. Add appendix A to subpart A to read as follows:

Appendix A to Subpart A of Part 37—Mobile Driver's License Issuance Infrastructure Requirements

A State that issues mDLs for acceptance by Federal agencies for official purposes as specified in the REAL ID Act must implement the requirements set forth in this appendix in full compliance with the cited references as set forth in the following table. All the standards identified in the following table are incorporated by reference, see § 37.4. If a State utilizes the services of a Delegated Third Party, the State must ensure the Delegated Third Party complies with all applicable requirements of this appendix for the services provided.

Section	Requirement
1: Certificate Authority Certificate Life-cycle Policy	
1.1	Maintain a Certificate Policy, which forms the State's Certificate System governance framework. If Certificate Systems are managed at a facility not controlled by the State, the State must require any Delegated Third Party to comply with the State's Certificate Policy. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; • CA Browser Forum Network and Certificate System Security Requirements; • NIST SP 800-57 Part 1, Rev. 5; • NIST SP 800-57 Part 2, Rev. 1; • NIST SP 800-57 Part 3, Rev. 1; • NIST 800-53 Rev. 5, AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PL-8, PL-10, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1; and • NIST SP 800-53B.
1.2	Perform management and maintenance processes which includes baseline configurations, documentation, approval, and review of changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front End and Internal Support Systems. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.IP-3; and

Section	Requirement
	• NIST SP 800-53 Rev. 5, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-8, CM-9, CM-10, CM-11, CM-12, MA-2, MA-3, MA-4, MA-5, MA-6, PE-16, PE-17, PE-18, PL-10, PL-11, RA-7, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-11, SA-15, SA-17, SA-22, SC-18, SI-6, SI-7, SR-2, SR-5.
1.3	Apply recommended security patches, to Certificate Systems within six months of the security patch's availability, unless the State documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework ID.RA-1, PR.IP-12; and • NIST SP 800-53 Rev. 5, SI-2, SI-3.
2: Certificate Authority Access Management	
2.1	Grant Administration access to Certificate Systems only to persons acting in Trusted Roles, and require their accountability for the Certificate System's security, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-4; and • NIST SP 800-53 Rev. 5, AC-1, AC-2, AC-3, AC-5, AC-6, AC-8, AC-21, AC-22, AC-24, CA-6, PS-6.
2.2	Change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-1; and • NIST SP 800-53 Rev. 5, AC-1, AC-2, AC-3, AC-6, IA-1, IA-2, PS-4, PS-5.
2.3	Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-1; and • NIST SP 800-53 Rev. 5, AC-1, AC-2, AC-3, AC-5, AC-6, IA-1, IA-2.
2.4	Document the responsibilities and tasks assigned to Trusted Roles and implement "separation of duties" for such Trusted Roles based on the security-related concerns of the functions to be performed, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements;

Section	Requirement
	• NIST Cybersecurity Framework - PR.AC-4; and • NIST SP 800-53 Rev. 5, AC-1, AC-2, AC-5, AC-6, MP-2, PS-9.
2.5	Restrict access to Secure Zones and High Security Zones to only individuals assigned to Trusted Roles, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC; and • NIST SP 800-53 Rev. 5, AC-1, AC-2, AC-3, AC-5, AC-6, MP-2, PS-1, PS-6.
2.6	Restrict individuals assigned to Trusted Roles from acting beyond the scope of such role when performing administrative tasks assigned to that role, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-1, PR.AC-4, PR.AC-6, PR.AT-2; and • NIST SP 800-53 Rev. 5,, AT-2, AT-3, PM-13, PM-14.
2.7	Require employees and contractors to observe the principle of “least privilege” when accessing or configuring access privileges on Certificate Systems, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-4, PR.AC-2; and • NIST SP 800-53 Rev. 5, AC-1, AC-2, AC-3, AC-5, AC-6, PE-1, PE-3, PL-4
2.8	Require that individuals assigned to Trusted Roles use a unique credential created by or assigned to them in order to authenticate to Certificate Systems, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-1, PR.AC-6, PR.AC-4, PR.AC-7; and • NIST SP 800-53 Rev. 5, AC-1, IA-1, IA-2, IA-3, IA-5, IA-8, IA-12.
2.9	Lockout account access to Certificate Systems after a maximum of five failed access attempts, provided that this security measure: 1. Is supported by the Certificate System; 2. Cannot be leveraged for a denial-of-service attack; and 3. Does not weaken the security of this authentication control. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-7; and • NIST SP 800-53 Rev. 5, AC-7.

Section	Requirement
2.10	Implement controls that disable all privileged access of an individual to Certificate Systems within 4 hours of termination of the individual's employment or contracting relationship with the State or Delegated Third Party, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-7; and • NIST SP 800-53 Rev. 5, AC-1, AC-2, PS-1, PS-4, PS-7.
2.11	Implement Multi-Factor Authentication or multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework-PR.AC-6, PR.AC-7; and • NIST SP 800-53 Rev. 5, AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-11.
2.12	Implement Multi-Factor Authentication for all Trusted Role accounts on Certificate Systems, including those approving the issuance of a Certificate and Delegated Third Parties, that are accessible from outside a Secure Zone or High Security Zone, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-7; and • NIST SP 800-53 Rev. 5, AC-17, AC-18, AC-19, AC-20, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.
2.13	If Multi-Factor Authentication is used, implement only Multi-Factor Authentication that achieves an Authenticator Assurance Level equivalent to AAL2 or higher, in full compliance with the following references: • NIST SP 800-63-3 Section 4.3, 6.2; • NIST SP 800-63B; • NIST Cybersecurity Framework PR.AC-7; and • NIST SP 800-53 Rev. 5, IA-5, IA-7.
2.14	If multi-factor authentication is not possible, implement a password policy for Trusted Role accounts in full compliance with NIST SP 800-63B Section 5.1.1.2 Memorized Secret Verifiers and implement supplementary risk controls based on a system risk assessment.
2.15	Require Trusted Roles to log out of or lock workstations when no longer in use, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, AC-11, AC-12.

Section	Requirement
2.16	Configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user. A workstation may remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, AC-11, AC-12.
2.17	Review all system accounts at least every three months and deactivate any accounts that are no longer necessary for operations, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-1; and • NIST SP 800-53 Rev. 5, AC-2.
2.18	Restrict remote Administration or access to a State Issuing System, Certificate Management System, or Security Support System, including access to cloud environments, except when: 1. The remote connection originates from a device owned or controlled by the State or Delegated Third Party; 2. The remote connection is through a temporary, non-persistent encrypted channel that is supported by Multi-Factor Authentication; and 3. The remote connection is made to a designated intermediary device— a. located within the State's network or secured Virtual Local Area Network (VLAN), b. secured in accordance with the requirements of this appendix, and c. that mediates the remote connection to the Issuing System. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-3, PR.AC-7; and • NIST SP 800-53 Rev. 5, AC-17, AC-19, AC-20, IA-3, IA-4, IA-6.
3: Facility, Management, and Operational Controls	
3.1	Restrict physical access authorizations at facilities where Certificate Systems reside, including facilities controlled by a Delegated Third Party, by: 1. Verifying individual access authorizations before granting access to the facility; 2. Controlling ingress and egress to the facility using appropriate security controls; 3. Controlling access to areas within the facility designated as publicly accessible; 4. Escorting visitors, logging visitor entrance and exit from facilities, and limiting visitor activities within

Section	Requirement
	facilities to minimize risks to Certificate Systems; 5. Securing physical keys, combinations, and other physical access devices; 6. Maintaining an inventory of physical keys, combinations, and physical access devices; conduct review of this inventory at least annually; and 7. Changing combinations and keys every three years or when physical keys are lost, combinations are compromised, or when individuals possessing the physical keys or combinations are transferred or terminated. These Requirements must be implemented in full compliance with the following reference: • NIST SP 800-53 Rev. 5, PE-2, PE-3, PE-4, PE-5, PE-8.
3.2	Implement controls to protect Certificate System operations and facilities where Certificate Systems reside from environmental damage and/or physical breaches, including facilities controlled by a Delegated Third Party, in full compliance with the following reference: • NIST SP 800-53 Rev. 5, CP-2, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, PE-2, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-21.
3.3	If Certificate Systems are managed at a facility not controlled by the State, implement controls to prevent risks to such facilities presented by foreign ownership, control, or influence, in full compliance with the following reference: • NIST SP 800-53 Rev. 5, SR-2, SR-3, SR-4, SR-6.
3.4	Implement controls to prevent supply chain risks for Certificate Systems including: 1. Employing acquisition strategies, tools, and methods to mitigate risks; 2. Establishing agreements and procedures with entities involved in the supply chain of Certificate Systems; 3. Implementing an inspection and tamper protection program for Certificate Systems components; 4. Developing and implementing component authenticity policies and procedures; and 5. Developing and implementing policies and procedures for the secure disposal of Certificate Systems components. These requirements must be implemented in full compliance with the following reference: • NIST SP 800-53 Rev. 5, SR-5, SR-8, SR-9, SR-10, SR-11, SR-12.
4: Personnel Security Controls	

Section	Requirement
4.1	Implement and disseminate to personnel with access to Certificate Systems and facilities, including facilities controlled by a Delegated Third Party, a policy to control insider threat security risks that: 1. Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among State entities, and compliance; 2. Complies with all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 3. Designates an official in a Trusted Role to manage the development, documentation, and dissemination of the policy and procedures. These requirements must be implemented in full compliance with the following reference: • NIST SP 800-53 Rev. 5, MA-5, PS-1, PS-8.
4.2	Assign a risk designation to all organizational positions with access to Certificate Systems and facilities, in full compliance with the following reference: • NIST SP 800-53 Rev. 5, PS-2, PS-9.
4.3	Establish screening criteria for personnel filling organization positions with access to Certificate System and facilities, in full compliance with the following reference: • NIST SP 800-53 Rev. 5, PS-2, PS-3, SA-21.
4.4	Screen individual personnel in organizational positions with access to Certificate Systems and facilities, in full compliance with the following reference: • NIST SP 800-53 Rev. 5, PS-3.
4.5	Upon termination of individual employment, State or Delegated Third Party must: 1. Disable system access within 4 hours; 2. Terminate or revoke any authenticators and credentials associated with the individual; 3. Conduct exit interviews that include— a. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information, and b. Requiring terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process; 4. Retrieve all security-related organizational system-related property; and 5. Retain access to organizational information and systems formerly controlled by terminated individual. These requirements must be implemented in full compliance with the following reference: • NIST SP 800-53 Rev. 5, PS-4.
4.6	Review and update personnel security policy, procedures, and position risk designations at least once every 12 months, in full compliance with the following reference:

Section	Requirement
	• NIST SP 800-53 Rev. 5, PS-1, PS-2.
4.7	Provide training to all personnel performing Certificate System duties, on the following topics: 1. Fundamental principles of Public Key Infrastructure; 2. Authentication and vetting policies and procedures, including the State's Certificate Policy; 3. Common threats to Certificate System processes, including phishing and other social engineering tactics; 4. Role specific technical functions related to the administration of Certificate Systems; and 5. The requirements of this appendix. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.3.3; and • NIST SP 800-53 Rev. 5, CP-3, IR-2, SA-16.
4.8	Maintain records of training as required by section 4.7 of this appendix, in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Sections 5.3.3, 5.4.1; and • NIST SP 800-53 Rev. 5, AT-4.
4.9	Implement policies and processes to prevent any Delegated Third Party personnel managing Certificate Systems at a facility not controlled by a State from being subject to risks presented by foreign control or influence, in full compliance with the following reference: • NIST SP 800-53 Rev. 5, SR-3, SR-4, SR-6.
5: Technical Security Controls	
5.1	Segment Certificate Systems into networks based on their functional or logical relationship, such as separate physical networks or VLANs, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-5; and • NIST SP 800-53 Rev. 5, AC-4, AC-10, CA-3, CA-9, MP-3, MP-4, RA-2, RA-9, SC-2, SC-3, SC-4, SC-8.
5.2	Apply equivalent security controls to all systems co-located in the same network (including VLANs) with a Certificate System, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-5; and • NIST SP 800-53 Rev. 5, MP-5, MP-6, MP-7, RA-2, SC-7, SC-10, SC-39.

Section	Requirement
5.3	Maintain State Root Certificate Authority Systems in a High Security Zone and in an offline state or air-gapped from all other network operations. If operated in a cloud environment, State Root Certificate Authority Systems must use a dedicated VLAN with the sole purpose of Issuing Authority Certificate Authority (IACA) Root Certificate functions and be in an offline state when not in use for IACA Root Certificate functions. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, SC-32.
5.4	Protect IACA Root Certificate Private Keys using dedicated hardware security modules (HSMs), either managed on-premises or provided through cloud platforms, that are under Sole Control of the State or Delegated Third Party. These requirements must be implemented in full compliance with the following references: • NIST SP 800-57 Part 1, Rev. 5; • NIST FIPS 140-3; and • NIST SP 800-53 Rev. 5, SC-12, SC-13.
5.5	Protect Certificate Systems private keys using NIST FIPS 140-3 Level 3 or Level 4 certified HSMs, in full compliance with the following references: • NIST FIPS 140-3; and • NIST SP 800-53 Rev. 5, SC-12, SC-13.
5.6	Protect Document Signer Private Keys using HSMs, either managed on-premises or provided through cloud platforms, that are under Sole Control of the State or Delegated Third Party. These requirements must be implemented in full compliance with the following references: • NIST SP 800-57 Part 1, Rev. 5; • NIST FIPS 140-3; and • NIST SP 800-53 Rev. 5, SC-12, SC-13.
5.7	Protect Certificate Systems Document Signer keys using NIST FIPS 140-3 Level 2, Level 3, or Level 4 certified HSMs, in full compliance with the following references: • NIST FIPS 140-3; and • NIST SP 800-53 Rev. 5, SC-12, SC-13.
5.8	Maintain and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, SC-15, SC-20, SC-21, SC-22, SC-24, SC-28, SI-16.

Section	Requirement
5.9	Implement and configure, in full compliance with the following references: Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those Zones (including those with organizational business units that do not provide PKI-related services) and those on public networks. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, SC-15, SC-20, SC-21, SC-22, SC-24, SC-28, SI-16.
5.10	Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the State has identified as necessary to its operations. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, AC-4, SI-3, SI-8, SC-7, SC-10, SC-23, CM-7.
5.11	Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front End and Internal Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the State's or Delegated Third Party's operations and restricting use of such systems to only those that are approved by the State or Delegated Third Party. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.PT-3; and • NIST SP 800-53 Rev. 5, CM-7.
5.12	Implement Multi-Factor Authentication on each component of the Certificate System that supports Multi-Factor Authentication, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework PR.AC-7; and • NIST SP 800-53 Rev. 5, IA-2.
5.13	Generate IACA Root Certificate Key Pairs with a documented and auditable multi-party Key Ceremony, performing at least the following steps: 1. Prepare and follow a Key Generation Script; 2. Require a qualified person who is in a Trusted Role and not a participant in the key generation to serve as a live witness of the full process of generating the IACA Root Certificate Key Pair, or record a video in lieu of a live witness; 3. Require the qualified witness to issue a report confirming that the State followed its Key ceremony

Section	Requirement
	during its Key and Certificate generation process, and confirming that controls were used to protect the integrity and confidentiality of the Key Pair; 4. Generate the IACA Root Certificate Key Pair in a physically secured environment as described in the State's Certificate Policy and/or Certification Practice Statement; 5. Generate the IACA Root Certificate Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge. IACA Root Certificate Key Pair generation requires a minimum of three persons, consisting of two key generation ceremony administrators and one qualified witness); 6. Log the IACA Root Certificate Key Pair generation activities, sign the witness report (and video file, if applicable), with a document signing key which has been signed by the IACA Root Certificate Private Key, and include signed files and document signing public certificate with the IACA Root Certificate Key Pair generation log files; and 7. Implement controls to confirm that the IACA Root Certificate Private Key was generated and protected in conformance with the procedures described in the State's Certificate Policy and/or Certification Practice Statement and the State's Key Generation Script. These Requirements must be implemented in full compliance with the following reference: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Section 6.1.1.1.
5.14	Generate Document Signer Key Pairs with a documented and auditable multi-party Key Ceremony, performing at least the following steps: 1. Prepare and follow a Key Generation Script; 2. Generate the Document Signer Key Pairs in a physically secured environment as described in the State's Certificate Policy and/or Certification Practice Statement; 3. Generate the Document Signer Key Pairs using only personnel in Trusted Roles under the principles of multiple person control and split knowledge, using at least two key generation ceremony administrators; 4. Log the Document Signer Key Pairs generation activities; and 5. Implement controls to confirm that the Document Signer Private Key was generated and protected in conformance with the procedures described in the State's Certificate Policy and/or Certification Practice Statement and the State's Key Generation Script. These Requirements must be implemented in full compliance with the following reference: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Section 6.1.1.1.
6: Threat Detection	

Section	Requirement
6.1	Implement a System under the control of State or Delegated Third Party Trusted Roles that continuously monitors, detects, and alerts personnel to any modification to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems, unless the modification has been authorized through a change management process. The State or Delegated Third Party must respond to the alert and initiate a plan of action within at most 24 hours. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • NIST Cybersecurity Framework DE.CM-7; and • NIST SP 800-53 Rev. 5, CA-7, CM-3, SI-5.
6.2	Identify any Certificate Systems under the control of State or Delegated Third Party Trusted Roles that are capable of monitoring and logging system activity, and enable those systems to log and continuously monitor the events specified in section 7 of this appendix. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, AU-12.
6.3	Monitor the integrity of the logging processes for application and system logs using either continuous automated monitoring and alerting, or human review, to confirm that logging and log-integrity functions meet the requirements set forth in section 7 of this appendix. Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 days. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; and • NIST SP 800-53 Rev. 5, AU-1, AU-6, AU-5, AU-9, AU-12.
7: Logging	
7.1	Log records must include the following elements: 1. Date and time of record; 2. Identity of the person or non-person entity making the journal record; and 3. Description of the record. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.1; • NIST Cybersecurity Framework PR.PT-1; and • NIST SP 800-53 Rev. 5, AU-2, AU-3, AU-8.

Section	Requirement
7.2	Log at least Certificate System and key lifecycle events for IACA Root Certificates, Document Signer Certificates, and other intermediate certificates, including: 1. Key generation, backup, storage, recovery, archival, and destruction; 2. Certificate requests, renewal, and re-key requests, and revocation; 3. Approval and rejection of certificate requests; 4. Cryptographic device lifecycle management events; 5. Generation of Certificate Revocation Lists and OCSP entries; 6. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles; 7. Issuance of Certificates; and 8. All verification activities required in section 2 of this appendix and the State's Certification System Policy. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.1; • NIST Cybersecurity Framework PR.PT-1; and • NIST SP 800-53 Rev. 5, AU-1, AU-2, AU-3, AU-4, AU-7, AU-10, SC-17.
7.3	Log Certificate System Security events, including: 1. Successful and unsuccessful PKI system access attempts; 2. PKI and security system actions performed; 3. Security profile changes; 4. Installation, update and removal of software on a Certificate System; 5. System crashes, hardware failures, and other anomalies; 6. Firewall and router activities; and 7. Entries to and exits from the IACA facility if managed on-premises. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.1; and • NIST SP 800-53 Rev. 5, AU-2, AU-3, AU-4, AU-7, AU-10, CM-3, PE-6, SI-11, SI-12.
7.4	Maintain Certificate System logs for a period not less than 36 months, in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.3; and • NIST SP 800-53 Rev. 5, AU-4, AU-10, AU-11.

Section	Requirement
7.5	Maintain IACA Root Certificate and key lifecycle management event logs for a period of not less than 24 months after the destruction of the IACA Root Certificate Private Key, in full compliance with the following references: • CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Section 5.4.3; • NIST Cybersecurity Framework PR.PT-1; and • NIST SP 800-53 Rev. 5, AU-2, AU-4, AU-10, AU-11.
8: Incident Response & Recovery Plan	
8.1	Implement automated mechanisms under the control of State or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • National Cyber Incident Response Plan; • NIST Cybersecurity Framework RS.CO-5, RS.AN-5; and • NIST SP 800-53 Rev. 5, AU-1, AU-2, AU-6, IR-5, SI-4, SI-5.
8.2	Require Trusted Role personnel to follow up on alerts of possible Critical Security Events, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • National Cyber Incident Response Plan; and • NIST SP 800-53 Rev. 5, AC-5, AC-6, IR-1, IR-4, IR-7, SI-4, SI-5.
8.3	If continuous automated monitoring and alerting is utilized, respond to the alert and initiate a plan of action within 24 hours, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • National Cyber Incident Response Plan; and • NIST SP 800-53 Rev. 5, IR-1, PM-14, SI-4.
8.4	Implement intrusion detection and prevention controls under the management of State or Delegated Third Party individuals in Trusted Roles to protect Certificate Systems against common network and system threats, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • CISA Cybersecurity Incident & Vulnerability Response Playbooks; • National Cyber Incident Response Plan; • NIST Cybersecurity Framework DE.AE-2, DE.AE-3; DE.DP-1; and

Section	Requirement
	• NIST SP 800-53 Rev. 5, IR-1, IR-4, IR-7, IR-8, SI-4, SI-5.
8.5	Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • CISA Cybersecurity Incident & Vulnerability Response Playbooks; • National Cyber Incident Response Plan; • NIST Cybersecurity Framework PR.IP-9; and • NIST SP 800-53 Rev. 5, CA-5, CP-2, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, SI-1, SI-2, SI-10.
8.6	Within 72 hours of the discovery of a significant cyber incident or breach which may compromise the integrity of the Certificate Systems, provide written notice to TSA of the incident or breach at www.dhs.gov/real-id/mDL. These Requirements must be implemented in full compliance with the following references: • National Cyber Incident Response Plan; and • NIST SP 800-53 Rev. 5, IR-6.
8.7	Undergo a Vulnerability Scan on public and private IP addresses identified by the State or Delegated Third Party as the State's or Delegated Third Party's Certificate Systems at least every three months, and after performing any significant system or network changes. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • National Cyber Incident Response Plan; and • NIST SP 800-53 Rev. 5, CM-1, CM-4, IR-3, RA-1, RA-5.
8.8	Undergo a Penetration Test on the State's and each Delegated Third Party's Certificate Systems at least every 12 months, and after performing any significant infrastructure or application upgrades or modifications. These Requirements must be implemented in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • National Cyber Incident Response Plan; • NIST Cybersecurity Framework PR.IP-7; and • NIST SP 800-53 Rev. 5, CA-2, CA-8, CM-4, RA-3.
8.9	Record evidence that each Vulnerability Scan and Penetration Test was performed by a person or entity with the requisite skills, tools, proficiency, code of ethics, and independence.

Section	Requirement
8.10	Review State and/or Delegated Third Party Incident Response & Recovery Plan at least once during every 12 months to address cybersecurity threats and vulnerabilities, in full compliance with the following references: • CA Browser Forum Network and Certificate System Security Requirements; • National Cyber Incident Response Plan; and • NIST SP 800-53 Rev. 5, CP-2, IR-1, IR-2, SC-5.

Dated: August 17, 2023.

David P. Pekoske,

Administrator.

[FR Doc. 2023-18582 Filed: 8/28/2023 4:15 pm; Publication Date: 8/30/2023]